FROM CONCEPTION TO BIRTH: THE FORCES RESPONSIBLE FOR AFCYBER'S EVOLUTION

BY

JOHANNES MOORE

A THESIS PRESENTED TO THE FACULTY OF

THE SCHOOL OF ADVANCED AIR AND SPACE STUDIES

FOR COMPLETION OF GRADUATION REQUIREMENTS

SCHOOL OF ADVANCED AIR AND SPACE STUDIES

AIR UNIVERSITY

MAXWELL AIR FORCE BASE, ALABAMA

JUNE 2014

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
JUN 2014		**00-00-2014 to 00-00-2014**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
From Conception To Birth: The Forces Responsible For AFCyber's Evolution	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **School of Advanced Air And Space Studies,,Air University,,Maxwell Air Force Base,,AL**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

In 2005, SECAF Wynne and CSAF General Moseley acknowledged the growing threat to national security posed through the cyber domain and recognized the need for the USAF to embrace the still-chaotic world of ???cyber.??? After amending the USAF Mission Statement in 2005, he tasked Lieutenant General Robert Elder, 8 AF/CC, to devise an organizational structure for a cyber-focused Major Command (MAJCOM). Some outside the service perceived this as a mission grab by the USAF while others within the Air Force questioned the decision to create a Major Command focused on the cyber domain. Lt Gen Elder successfully built an ???on-ramp??? for the new MAJCOM, but an organizational crisis resulted in the creation of a cyber-focused Numbered Air Force rather than a cyber-focused Major Command. After this change, Lt Gen Elder and Major General William Lord (AFCYBER's Provisional Commander) hired a team to develop how cyber operations would contribute in concept and execution toward joint operations. This thesis describes in unprecedented detail the evolution of AFCYBER, identifies the USAF's response to the bureaucratic challenges, and assesses the organizational response to the sweeping SECAF-directed changes.

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**105**	

APPROVAL

The undersigned certify that this thesis meets master's-level standards of research, argumentation, and expression.

_____

MARK O. YEISLEY (Date)

_____

MICHAEL V. SMITH (Date)

DISCLAIMER

The conclusions and opinions expressed in this document are those of the author. They do not reflect the official position of the US Government, Department of Defense, the United States Air Force, or Air University.

ABOUT THE AUTHOR

Major Johannes Moore earned his commission in 2000 through the Air Force Reserve Officer Training Corps program at University of Miami, Florida. He completed the Intelligence Officer Course in 2003. From 2003 through 2012, Major Moore served in several roles, including: Flight Commander, Intelligence Analyst, and Deputy Chief of an Air Operations Center ISR Division. He has participated in multiple combat deployments in support of Operations ENDURING FREEDOM and IRAQI FREEDOM, NATO's Training Mission-Iraq, and NATO's Operation JOINT GUARDIAN in Kosovo. Major Moore holds a bachelor's degree in Criminal Justice from Florida International University, a master's degree in Business Administration from Trident University, a master's degree in Military Operational Art and Science from Air Command and Staff College, and a master's of philosophy in Military Strategy from the School of Advanced Air and Space Studies.

ACKNOWLEDGEMENTS

I offer my sincere thanks to my thesis advisor, Colonel Mark Yeisley, for his remarkable support during this project. His efforts were crucial to this paper's successful completion and his affable demeanor and wit added much-needed levity to the writing process. I also offer my appreciation to Colonel Rick Bailey who, with Colonel Yeisley, offered both personal and professional advice throughout the SAASS program. Our conversations about officership, family, and "real life" had an even bigger impact on me than their instructorship. Additionally, I wish to thank my thesis reader, Colonel Michael Smith, for the insightful inputs that helped me cross the metaphorical finish line. I owe a great deal to Ms. Sheila McKitt, who helped me navigate much of the Air Force's institutional "administrivia" and allowed me to focus on my academics. Lastly, my gratitude goes to the members of the SAASS faculty; the persistent challenge of meeting the high standards throughout the 11-month curriculum made me both a better scholar and a better officer. This opportunity to spend a year "thinking about thinking" has been a remarkable one, but the all-star SAASS faculty has made it even better than expected.

In addition to the brilliant instructors on staff, I owe thanks to every individual that helped me develop this thesis. Colonel Stephen "Lux" Luxion provided the seed corn that eventually became this thesis. Dr. Greg Ball (24 AF Historian) and Lane Calloway (8 AF Historian) provided dozens of documents that allowed me to build the skeleton for this important story. Generals "Norty" Schwartz, Ron Keys, Bob Elder, Bill Lord, and B.J. Shwedo devoted countless hours providing me documents, speaking with me, and emailing me stray thoughts that would form the narrative of this important piece of history. Colonel David "Driver" Fahrenkrug provided important "behind-the-scenes" details from his time on the Eighth Air Force staff. Dr. Lani Kass and Colonel Forrest Hare of the Cyberspace Task Force gave me access to their insights as well as to several general officers I could not have reached otherwise.

My classmates were a great help to me throughout the course. In particular, Raj Agrawal, "Sinna" Bonn, "Tapper" Dailey, "Puck" Neitzke, and "Sputnik" Vollkommer provided a network of support when writing papers, preparing for the SAASS comprehensive final, and attempting to link concepts from across blocks of instruction. Additionally, "Pint" Maguinness, though she will deny it, provided me more mentorship and friendship than I deserved.

Lastly, I could not have completed this thesis without my family's steadfast support. My wonderful children were incredibly understanding

despite my absenteeism for much of the last year. Most importantly, I thank my wife. She set aside many of her own goals to support our family while I underwent the rigors of SAASS. No matter how good or bad my days were – and I experienced a fair number of both during the 11-month course – she provided a shoulder to cry on, a sympathetic ear, or a high-five as the situation merited. She is the cornerstone of our family, and without her, my children and I would be lesser people.

ABSTRACT

In 2005, SECAF Wynne and CSAF General Moseley acknowledged the growing threat to national security posed through the cyber domain and recognized the need for the USAF to embrace the still-chaotic world of "cyber." After amending the USAF Mission Statement in 2005, he tasked Lieutenant General Robert Elder, 8 AF/CC, to devise an organizational structure for a cyber-focused Major Command (MAJCOM). Some outside the service perceived this as a "mission grab" by the USAF, while others within the Air Force questioned the decision to create a Major Command focused on the cyber domain. Lt Gen Elder successfully built an "on-ramp" for the new MAJCOM, but an organizational crisis resulted in the creation of a cyber-focused Numbered Air Force rather than a cyber-focused Major Command. After this change, Lt Gen Elder and Major General William Lord (AFCYBER's Provisional Commander) hired a team to develop how cyber operations would contribute in concept and execution toward joint operations. This thesis describes in unprecedented detail the evolution of AFCYBER, identifies the USAF's response to the bureaucratic challenges, and assesses the organizational response to the sweeping SECAF-directed changes.

CONTENTS

Illustrations

Figures

Chapter 1

Introduction

The United States Air Force (USAF) boldly changed her mission statement in 2005, adding "cyberspace" as a domain in which the service would deliver effects in defense of the United States.[1] The new version presented by Secretary of the Air Force (SECAF) Michael W. Wynne and Chief of Staff of the Air Force (CSAF) General T. Michael Moseley reads "The mission of the United States Air Force is to deliver sovereign options for the defense of the United States of America and its global interests-to fly and fight in Air, Space, and Cyberspace."[2] This mission statement reflected the service's intent to organize, train, and equip forces to operate in the cyberspace domain, despite the fact that, in 2005, the Department of Defense (DOD) had not officially declared cyberspace a domain. The service spent the next four years planning, creating, and building an organization to deliver effects in this manmade domain in support of United States combatant and joint force commanders. Twenty-fourth Air Force (24 AF) is the result of those years of work, but the organization is much different from the one that began to take shape in 2006 and 2007. This thesis describes the evolution of Air Forces Cyber (AFCYBER) from its genesis in 2006 to 24th Air Force's Final Operational Capability (FOC) declaration in 2010.[3]

Chapter 2 describes the evolution of the cyber domain in the 20 years leading up to the USAF Mission Statement change. It explains

[1] Air Force Document (AFD) 111003-050, *Letter to the Airmen of the United States Air Force*, 07 December 2005, http://www.24af.af.mil/shared/media/document/AFD-111003-050.pdf (accessed 01 January 2014).
[2] *Letter to the Airmen of the United States Air Force*, 07 December 2005.
[3] General C. Robert Kehler, Commander, Air Force Space Command, to Commander, United States Strategic Command, memorandum, 01 October 2010. AFD-111003-057; Scott Fontaine, "Major Command, 24th AF Reach Full Capability," *Air Force Times,* 04 October 2010, www.airforcetimes.com/article/20101004/NEWS/10040322/Major-command-24th-AF-reach-full-capability (accessed 01 January 2014).

the steady progression of cyber incidents to demonstrate the growing threat to national security. It also describes the effects of frequent US policy changes and the slow build-up of US government (USG) and military organizations devoted to securing the cyber domain. These events provide the context for the USAF's reorganization to improve the service's capability to enable it to "fly, fight, and win in air, space, and cyberspace."

Chapter 3 describes the USAF intent to ensure freedom of movement in cyberspace by operationalizing the domain. This operationalization began with changing the USAF Mission Statement in 2005 and continued with the order that Eighth Air Force "develop an 'on ramp' to transition the MIGHTY EIGHTH into a MAJCOM Component responsible for integrated global effects, both kinetic and non-kinetic."[4] During the 24 months following General Moseley's "Go Do Letter," Lieutenant General Elder and his Eighth Air Force team worked to develop the organizational and functional framework for the USAF's first new Major Command (MAJCOM) in 25 years. This MAJCOM was intended to demonstrate that the USAF was serious about information assurance and cyberspace superiority to Congress, the joint community, as well as airmen who traditionally thought of communications career fields as "enablers." Throughout this process, many felt that a cyber-focused MAJCOM was the wrong type of organization to train cyber forces. General Elder's work somewhat supported this position, but the decision to create a cyber Numbered Air Force (NAF) rather than a MAJCOM was not made until after the organizational crisis which culminated with the forced resignation of General Moseley and Secretary Wynne.

Chapter 4 explains the organizational dynamics that resulted in a cyber-focused NAF. The new Chief and Secretary almost immediately

[4] General T. Michael Moseley, Chief of Staff of the Air Force, to Lieutenant General Robert J. Elder, Jr., Commander, Eighth Air Force, memorandum, 01 November 2006. AFD-111003-055.

suspended all planning for the cyber MAJCOM and ultimately decided that a Numbered Air Force was a more appropriate organization to organize, train, and equip forces while also properly presenting these forces to joint commanders to prosecute warfighting objectives. Although the new organization, 24 AF, largely followed the blueprint passed to them by Lt Gen Elder, the organization is much weaker than the one envisioned by Secretary Wynne in 2005.

Lastly, this study provides the conclusions drawn from these events and the resultant implications. Nearly a decade after the new USAF Mission Statement, chaos and misunderstanding continues to reign in the cyber domain. The Air Force is not certain of its ability to guarantee freedom of movement in cyberspace, let alone the ability to gain and maintain cyberspace superiority. Ultimately, Chapter 5 demonstrates that the decision to organize cyber forces in a Numbered Air Force subordinate to Air Force Space Command was the result of organizational bargaining. Although some argue that the results of these bargains have resulted in a watered down USAF cyber capability, there is little evidence that a cyber-focused Major Command would solve this problem any more effectively than 24 AF.

Existing Literature

Despite the importance of "cyber" as an emerging domain and mission set, the body of work describing the creation of an Air Force higher headquarters charged with organization, training, and equipping forces to "fly and fight" in this domain is relatively small. Major Leland Bohanon's 2008 School of Advanced Air and Space Studies (SAASS) thesis, *Cyberspace and the New Age of Influence*, devoted some pages to Lieutenant General Elder's quest to build a "major command that would bring a war-fighting capability to the cyberspace domain."[5] This

[5] Major Leland Bohannon, *Cyberspace and the New Age of Influence* (Master's thesis, School of Advanced Air and Space Studies, June 2008), 3.

provided a good, though modest, introduction to the United States Air Force's early embrace of cyber as an emerging mission set; however, Major Bohanon's thesis did not explore the service's reorganization. Instead, his study advanced "a theory for operations in cyberspace that uses the cyber domain to strategically influence an adversary in a context prior to armed conflict."[6]

Similarly, in their 2008 Air War College thesis titled *Presentation of AFCYBER Forces: A Hybrid Approach*, Colonels Brooks, Zucco, Worley, and Davis describe some models they felt the United States Air Force should consider when presenting cyber forces to a combatant commander.[7] After examining the Space, Air Mobility, and Special Operations models, these officers present their own hybrid approach. This thesis was well-written and a wonderful source; however, it was intended to be more speculative than retrospective. Majors Susan Magaletta and Todd Stratton professionally addressed similar issues in their Air Command and Staff College (ACSC) theses (*Command Relationships of Cyberspace Forces* and *Organization of Cyberspace Forces*, respectively).[8] Written in 2008, these documents offered options on how an AFCYBER organization should ultimately be designed, but did little to describe the path 8 AF and 24 AF ultimately selected, nor did they provide senior leader insight into the decisions that led the USAF down that path.

The 24th Air Force Heritage Pamphlet was an outstanding resource, as it provided an objective timeline of major milestones between the aforementioned 2005 USAF Mission Statement change to General Kehler's (Commander, Air Force Space Command) 2010

---

[6] Bohannon, *Cyberspace and the New Age of Influence*.

[7] Colonel Todd A. Brooks et al., *Presentation of AFCYBER Forces: A Hybrid Approach* (Master's thesis, Air War College, 24 February 2008).

[8] Major Susan E. Magaletta, *Command Relationships of Cyberspace Forces* (Master's thesis, Air Command and Staff College, April 2008); Major Todd R. Stratton, *Organization of Cyberspace Forces* (Master's thesis, Air Command and Staff College, April 2008).

declaration that 24th Air Force was fully operationally capable.[9] Unfortunately, this pamphlet provided limited details about the organization of AFCYBER, Lieutenant General Elder's plan for the headquarters in 2006 and 2007, and the decisions made by senior leaders that resulted in the current AFCYBER design and her place in the Air Force chain of command. This is not a criticism of that document. On the contrary, the 24th Air Force Historian Office's documentation was critical to this author's understanding of the major events resulting in the creation of AFCYBER.

This thesis adds to the body of literature on Air Forces Cyber and Eighth Air Force through rigorous analysis of key stakeholders and events. It examines circumstances surrounding the Air Force's decision to add "cyber" to the list of domains for which the USAF is responsible as well as the choice to "[e]stablish AFCYBER to develop and consolidate robust cyber-dominance capabilities that provide interdependent air, space, and cyberspace warfighting options to the Joint Force Commander."[10] It then analyzes the major decisions made by Lieutenant General Elder and Major General William T. Lord (Provisional Commander, AFCYBER) in 2006-07. My objective is to examine the people and decisions that shaped the Air Force's view of what a cyber organization should look like, then scrutinize the effects these people and decisions had on the ultimate development of 24th Air Force, Air Forces Cyber.

Primary Sources of Evidence

Three data sources provide the bulk of the evidence in support of this objective. First, documents such as Program Action Directives (PADs), official memoranda, white papers, and working documents are

[9] Gregory W. Ball, PhD, *A Brief History of the 24th Air Force,* 15 October 2012.AFD-121219-034. http://www.24af.af.mil/shared/media/document/AFD-121219-034.pdf (accessed 01 January 2014)
[10] Headquarters United States Air Force Program Action Directive 07-08, Change 1, *Implementation of the Secretary of the Air Force direction to Establish Air Force Cyberspace Command (AFCYBER)*, January 2008, Para 1.1, page 1.

stored at the Historical Research Agency (HRA) at Maxwell Air Force Base in Montgomery, Alabama. This collection is invaluable due to its objectivity and clear communication of senior leaders' policy positions. The information provided therein enabled the author to create a timeline of events to act as a starting point for the personal narrative.

The second set of evidentiary sources is a collection of interviews with the officers involved with the development of AFCYBER. Some of these interviews are part of the United States Air Force Oral History Program, the transcripts of which are housed at the Air Force's HRA. Interviews with General (ret) Norton A. Schwartz, Major General (sel) Bradford J. Shwedo, and Colonel David Fahrenkrug, however, were conducted by the author with the specific intent of learning more about how and why Air Forces Cyber developed the way that it did. "Cyber interviews" conducted via email with General (ret) Ronald E. Keys, Lieutenant General (ret) Elder Robert J. Elder, Jr., Lieutenant General (ret) William T. Lord, Major General (ret) John M. Maluda, Colonel Forrest Hare, and Dr. Lani Kass were conducted for similar reasons with great success.

Lastly, the 8th Air Force Historian, Mr. William "Lane" Calloway, and the 24th Air Force Historian, Dr. Gregory Ball, provided critical documentation. Their exquisite record-keeping and willingness to share even obscure staff summary sheets and PowerPoint presentations ensured historical accuracy despite occasional contradictions among those interviewed by the author.

Chapter 2

The Growing Cyber Threat

In 2006, the United States Air Force (USAF) senior leadership decided to build a four-star headquarters devoted to consolidating "AF-unique cyber capabilities and… executing… the full spectrum of integrated global effects (kinetic and non-kinetic)."[1] This announcement indicates that then-Secretary of the Air Force Michael W. Wynne and then-Chief of Staff of the Air Force T. Michael Moseley understood that the cyber domain posed a significant threat to US national security. This chapter highlights this ever-increasing threat by describing key cyber-attacks in recent history. Although the intentions of some of these attacks are clear, for many attacks, the agent and the motive remain a mystery. This uncertainty, both in terms of attribution and motive, is a routine characteristic of cyber-attacks. This provides some relief for the agents performing the attack while frustrating those suffering the attack.

This chapter also explains some United States government (USG) policy changes and organizations created to address the increased cyber threats in the two decades leading up to the announced creation of Air Forces Cyber (AFCYBER) Major Command (MAJCOM). Throughout the chapter, the complexity and uncertainty that exists due to the cyber domain is clear; in fact, the uncertainty appears be increasing with the passage of time and the increasing number of cyber tools available to those with the intent and capability to use them. By the end of the chapter, the reader will have a better understanding of the national security environment as it relates to cyber operations. This will aid the

[1] Josh Rogin, "Air Force To Create Cyber Command," *FCW: The Business of Federal Technology,* 13 November 2006. http://fcw.com/articles/2006/11/13/air-force-to-create-cyber-command.aspx (accessed 04 February 2014);General T. Michael Moseley, CSAF, to 8 AF/CC, memorandum, 07 November 2006, "Operational Cyber Command 'Go Do' Letter," http://www.24af.af.mil/shared/media/document/AFD-111003-055.pdf (accessed 05 February 2014).

reader in understanding the context that led to the organizational changes experienced by the USAF between 2005 and 2009.

Cyber-attacks: Who Needs A Gun When You Have a Keyboard?

The internet first gained widespread popularity in the 1990s, but governments and private companies began relying on computer hardware and software to control and regulate important systems as early as the 1960s and 1970s.[2] By the 1980s, computers were critical in the regulation of nearly every large-scale engineering project. Soon, banks, commercial and private companies, and governments relied on computers and the cyber domain to conduct operations. While the cyber domain served as an enabler, it also increased the risk posed by individuals and groups with both the malicious intent and the capability to interfere with these operations. Not only is it difficult to identify who is conducting a cyber-attack, it is often difficult to assess the purpose behind a cyber-attack. Sometimes, the goal is clear: in these cases, the objective is typically profit, espionage (both commercial and government), or the deliberate weakening of a competitor. Other times, however, the goal is less certain. The cases described below provide examples of the capabilities, vulnerabilities, and uncertainties in the cyber domain. Notably, with only occasional exceptions, the attacks have become more frequent and more damaging with the passage of time. This is due largely to the increased reliance on the cyber domain and the resulting increase in vulnerabilities, as well as the improved skill levels of those performing the attacks.

[2] For instance, the US Department of Interior's Bureau of Reclamation began computer (digital) automation of power generation in the early 1970s. These projects included 58 dams, power plants, and canals across the nation. Chau Nguyen and Terry Bauman, "Hoover Dam Modernization Project First of Its Kind," Hydropower Reform Coalition, 2009. http://www.hydroreform.org/sites/default/files/Nguyen_Hoover_Dam_Modernization.pdf (accessed 08 April 2014).

1982 – Sabotage and The Three-Kiloton "Logic Bomb."[3] In the early 1980s, the Soviet Union struggled to develop the technologies necessary to build modern infrastructure for the state-owned Russian oil and gas industries. Specifically, the Soviets lacked the technology of the automated pump and valve controls necessary to manage thousands of miles of pipeline. Compounding the problem, Western nations refused to sell the desired technology to the communist government. The KGB, the Soviet intelligence agency, was tasked to steal Western technologies. The Central Intelligence Agency (CIA) discovered this plot, and responded with "a massive program to ensure that the Soviets were able to steal the technologies they need, but the CIA introduced a series of minor errors into the designs."[4] The stolen control software, tainted with the CIA's "logic bomb," caused the Urengoy–Surgut–Chelyabinsk natural gas pipeline to malfunction and resulted in a three-kiloton explosion and resultant fire that was visible from space. This was the most massive non-nuclear explosion ever recorded. Thomas C. Reed, former Secretary of the Air Force and Director of the National Reconnaissance Office, wrote, "NORAD feared a missile liftoff from a place where no rockets were known to be based. Or perhaps it was the detonation of a small nuclear device… [but] they had detected no electromagnetic pulse, characteristic of nuclear detonations."[5]

This is the first assessed major cyber-attack in history, and is perhaps the first battle between two nations in the cyber domain, though (characteristic of cyber-attacks) no entity has ever claimed credit for the attack. No subsequent attacks have had such a

---

[3] A *logic bomb* is a computer program often hidden within another seemingly innocuous program that is designed to perform malicious actions when certain conditions have been met. Merriam-Webster, *Merriam-Webster's Collegiate Dictionary.* (Springfield, MA: Merriam-Webster, Inc., 2003), 732.

[4] Richard A. Clarke and Robert K. Knake, *Cyber War: The Next Threat to National Security and What to Do about It* (New York: Ecco, 2010), 93.

[5] Thomas C. Reed, *At the Abyss: An Insider's History of the Cold War* (Random House LLC, 2007), 269.

spectacular and destructive result, but some feel the threat today is greater than ever, and that the United States, with its unprecedented reliance on the cyber domain, is at greater risk than any other nation.[6]

1988 – Criminal Mischief and the Morris Worm.[7] In 1988, Cornell University graduate student Robert Tapan Morris, Jr. launched the first recognized worm onto the government's ARPAnet (the precursor to the internet).[8] The worm self-replicated and spread to more than half of the ARPAnet's 88,000 networked computers, slowing the university and government computers to the point of being unusable.[9] The 23-year-old Morris claimed he was merely attempting to measure the vastness of cyberspace, but the worm encountered a critical error and morphed into a virus that spread quickly, resulting in a massive denial of service with some damage estimates approaching $100 million. Cornell dismissed Morris from the school and he was the first person convicted under the 1987 Computer Fraud and Abuse Act.[10] The US Government sentenced Morris to three years' probation and fined him $10,000.[11] Morris now works at MIT's Computer Science and Artificial Intelligence Laboratory.[12]

This event may be the result of an unfortunate accident or intellectual curiosity gone awry, but demonstrated how easily a network

---

[6] Clarke and Knake, *Cyber War*, xiii & 261. Although some contend that Mr. Clarke is a bit of an alarmist, he has worked in four US Presidential administrations, including roles as the "National Coordinator for Security, Infrastructure Protection, and Counterterrorism" and "Special Advisor to the President on Cybersecurity." His personal access to three different Presidents lends credibility to some otherwise incredible assertions.

[7] A *worm* is a usually small self-contained and self-replicating computer program that invades computers on a network and usually performs a destructive action. Merriam-Webster, *Merriam-Webster's Collegiate Dictionary*, 1444.

[8] Jon Schiller, *Cyber Attacks & Protection: Civilization Depends on Internet & Email* (CreateSpace, 2010), 133.

[9] Staff, "Timeline: The U.S. Government and Cybersecurity," *Washington Post*, 16 May 2003, http://www.washingtonpost.com/wp-dyn/articles/A50606-2002Jun26.html (accessed 10 April 2014).

[10] *United States v. Robert Tapan Morris*, (United States Court of Appeals, Second Circuit), 07 March 1991. http://scholar.google.com/scholar_case?case=551386241451639668 (accessed 04 April 2014).

[11] Schiller, *Cyber Attacks & Protection*, 133.

[12] Faculty Biography, Massachusetts Institute of Technology. http://pdos.csail.mit.edu/rtm/ (accessed 04 April 2014).

could be penetrated and how quickly the exploited network could be affected. Following this incident, the General Accounting Office (GAO) asserted that the White House Science Advisor should be tasked with overseeing efforts to prevent future virus attacks.[13]

1994 – Hacking for Profit.[14] In 1994, a group of Russian hackers, led by Vladimir Levin, stole $10.7 million from Citibank by transferring the money into accounts set up by accomplices in Finland, the United States, the Netherlands, Germany and Israel. Levin appears to have gained access to the company's cash management system through unencrypted accounts, and the banking industry responded by improving cyber defenses.[15] Levin was eventually caught in London and extradited to the United States, where he was convicted of conspiracy to commit bank, wire, and computer fraud and sentenced to three years in prison.[16] The incident underscored the vulnerability of financial institutions in the early years of electronic transactions. The event also highlighted the potential profits available to those with marketable computing capabilities.

1998 – Espionage and MOONLIGHT MAZE. In March 1998, Department of Defense officials made an alarming discovery: since 1996, hackers were regularly accessing the computer network. During this series of cyber-attacks, the intruders accessed sensitive but unclassified data from the DOD, NASA, the Department of Energy, research labs, and private universities. James Adams, a member of the National Security Agency Advisory Board, confirmed the details of this

[13] Staff, "Timeline: The U.S. Government and Cybersecurity."
[14] To *hack* is to gain access to a computer illegally. Merriam-Webster, *Merriam-Webster's Collegiate Dictionary*, 559.
[15] Staff, "Notable Hacks," PBS Frontline, undated, http://www.pbs.org/wgbh/pages/frontline/shows/hackers/whoare/notable.html (accessed 29 March 2014).
[16] Staff, "Notable Hacks," PBS Frontline, undated.

intrusion in a 2001 issue of *Foreign Affairs* Magazine.[17] The hackers accessed military base and facility maps, US troop configurations, and encryption techniques. Additionally, US officials discovered "backdoor" tools that routed specific network traffic to Russian servers.[18] Adams suggested that this established precedents for future sabotage, but many issues remained unresolved. He claimed that the attacks originated from a Russian-registered internet protocol (IP) address, but no definitive evidence existed to prove the intrusion was state-sponsored and the Russian government pleaded ignorance.[19] The Pentagon reportedly did not "hack back" out of fear that inadvertently crippling the intruders' capabilities would be construed as acts of war, if the intruders were state-sponsored.[20]

Moonlight Maze was the first acknowledged cyber incident to target the US defense community, as well as the first reported case of large-scale cyber-espionage. Despite the power of the targeted state and the value and nature of the stolen information, attribution remained impossible. The United States could only issue a demarche to the Russian government and provided Russian officials with the telephone numbers from which the attacks appeared to be originating. Moscow said the numbers were inoperative and denied any prior knowledge of the attacks.[21]

---

[17] James Adams, "Virtual Defense," *Foreign Affairs,* May-June 2001, http://www.foreignaffairs.com/articles/57037/james-adams/virtual-defense (accessed 08 April 2014); Adams, "Virtual Defense," *Foreign Affairs,* May-June 2001.

[18] A *backdoor* in a computer system is a method of bypassing normal authentication, securing illegal remote access to a computer, or obtaining unauthorized access, while attempting to remain undetected. Wikipedia: "Backdoor Computing." http://en.wikipedia.org/wiki/Backdoor_(computing) (accessed 10 April 2014).

[19] James Adams, "Virtual Defense," *Foreign Affairs,* May-June 2001; An *IP address* is a numerical label assigned to each device (e.g., computer, printer) participating in a computer network that uses the Internet Protocol for communication. Wikipedia: "IP Address." http://en.wikipedia.org/wiki/IP_address (accessed 10 April 2014).

[20] Vernon Loeb, Washington Post, "Pentagon Hit with 'Maze' of Hack Attacks / Investigators Trace Case to Russia," *SFGate*, 07 May 2001, http://www.sfgate.com/news/article/Pentagon-hit-with-Maze-of-hack-attacks-2924284.php (accessed 10 April 2014).

[21] James Adams, "Virtual Defense," *Foreign Affairs,* May-June 2001.

1999 – Teenager Hacks USG. In mid-1999, 15-year-old Jonathan James penetrated the DOD computer network and installed a "backdoor" on its servers. This provided him ready access and enabled him to intercept thousands of sensitive emails, including ones containing usernames and passwords that allowed him access to other networks. James leveraged this access to hack into NASA software supporting the International Space Station's (ISS) environmental controls, including control of the humidity and temperature within the ISS living space.[22] NASA was forced to shut down their network for three weeks to remove the teenager's code and improve the integrity of the system. James's other targets included the Defense Threat Reduction Agency (DTRA), the DOD's official Combat Support Agency for countering weapons of mass destruction.[23] After authorities traced the access to the James family home, the boy was arrested and convicted of juvenile delinquency; the USG elected not to prosecute the teen as an adult under federal wiretap and computer abuse laws.[24]

Like Robert Morris, it appears that Jonathan James bore no ill will and had no malicious intent. However, the teenager was able to access the DOD network and computers critical to NASA's ISS operations, demonstrating how slow the USG was to protect its network and how a creative and skilled individual, regardless of age, appeared to have an advantage over the most powerful nation in the world. As the next example shows, James was not the only creative and skilled teenager in North America.

2000 – Canadian Teen Causes $1B Damage. In 2000, Michael Demon Calce, a 17-year-old from Quebec, hacked some of the most

---

[22] Solange Ghernaouti-Helie, *Cyber Power: Crime, Conflict and Security in Cyberspace* (CRC Press, 2013), 199.

[23] William Webb, *You've Been Hacked: 15 Hackers You Hope Your Computer Never Meets* (Absolute Crime, 2013).

[24] David Stout, "Youth Sentenced in Government Hacking Case," *The New York Times*, September 23, 2000, sec. U.S., http://www.nytimes.com/2000/09/23/us/youth-sentenced-in-government-hacking-case.html (accessed 08 April 2004).

secure online companies in the world. Over the period of one week, he attacked Yahoo, Dell, Amazon, E-Bay, and CNN using a denial of service attack in which he used approximately 200 university networks to bombard his targets.[25] Calce's actions resulted in about $1.2 billion in lost revenue for the affected companies.[26] Calce claimed he targeted these companies simply because he was challenged by another hacker.[27] Upon his arrest, he was sentenced to eight months of house arrest, a year of probation, and restricted use of the internet by the Montreal Youth Court. These DDoS attacks led to congressional hearings and legislative proposals aimed at closing security holes.[28]

This example demonstrates that even the largest internet companies in the world were penetrable from an outside cyber-attack in the early internet age. Although many contend that web security is better in 2014 than it was 15 years ago, Calce asserted in a recent interview that it is much easier to launch attacks today than it was then. A decade ago, a hacker had to work and build an arsenal of tools before launching an attack; now there are hacker desktops and ready-to-use tools that anyone can download, install, and implement.[29] Although hackers are infamous for hubris, the recently discovered "Heartbleed" bug demonstrates that 2014 networks are far from secure.[30]

---

[25] A denial-of-service (DoS) or distributed denial-of-service (DDoS) attack is an attempt to make a machine or network resource unavailable to its intended users. Although the means to carry out, motives for, and targets of a DoS attack may vary, it generally consists of efforts to temporarily or indefinitely interrupt or suspend services of a host connected to the Internet. "Denial-of-Service Attack," *Wikipedia, the Free Encyclopedia*, http://en.wikipedia.org/w/index.php?title=Denial-of-service_attack&oldid=603179829 (accessed 07 April 2014).

[26] Anthony Walsh and Craig Hemmens, *Introduction to Criminology* (SAGE, 2013), 460.

[27] Staff, "A Q&A with MafiaBoy," *Info Security Magazine*, 03 September 2013, http://www.infosecurity-magazine.com/view/34309/a-qa-with-mafiaboy/ (accessed 03 April 2014).

[28] Staff, "Timeline: The U.S. Government and Cybersecurity," Washington Post, 16 May 2003.

[29] Staff, "A Q&A with MafiaBoy," *Info Security Magazine*, 03 September 2013.

[30] Associated Press, "'Heartbleed' Bug Puts Internet Security at Risk," *Washington Post*, http://www.washingtonpost.com/posttv/business/technology/heartbleed-bug-puts-internet-security-at-risk/2014/04/10/99ddf5ce-be57-4f13-a62f-a0e05dc31cf9_video.html (accessed 11 April 2014).

2002 – Unattributed Attack on the Internet Itself. In 2002, during a DDOS attack lasting approximately one hour, seven of the 13 domain name system's root servers nearly crippled the entire internet. Called "the largest and most complex" attack in history, each server was bombarded with two to three times the load normally borne by the entire 13-server constellation; machines built to handle megabytes per second were flooded with 80 Mps of traffic. Seven servers were taken "completely down" and two others suffered "severe degradation."[31] Fortunately, the servers were designed to be somewhat redundant; if all 13 were forced offline, any application that uses domain names (such as e-mail and internet browsers) would have stopped functioning. Had the attack lasted longer than an hour, it likely would have brought the internet to a standstill.[32]

Despite an investigation spearheaded by the FBI and including the Department of Homeland Security (DHS), the attacker was never identified. This example demonstrates two critical elements of the cyber domain: the overall fragility of the internet (and cyber domain) itself as well as the challenges of attribution. When investigators cannot identify the perpetrators of "the largest and most complex" cyber-attack in history in order to bring them to justice, there is little to dissuade individuals and organizations with capability and willpower from acting with apparent impunity.

2004 – Titan Rain and Large-Scale Military Espionage. Beginning in the early 2000s, cyber intruders systematically scanned, attacked, and infiltrated USG networks. Although the attacks focused disproportionately on the DOD, the intrusions also targeted the

[31] Staff, "Feds Investigating 'Largest Ever' Internet Attack," ComputerWire, 23 October 2012, http://www.theregister.co.uk/2002/10/23/feds_investigating_largest_ever_internet/ (accessed 31 March 2014).
[32] Staff, "Top 10 Most Notorious Cyber Attacks in History," *ARN*, undated, http://www.arnnet.com.au/slideshow/341113/top_10_most_notorious_cyber_attacks_history/ (accessed 30 March 2014).

Departments of Energy, State, and Homeland Security, as well as NASA, Lockheed Martin, Sandia National Laboratories, and Redstone Arsenal.[33] Unfortunately, the US did not detect the series of attacks until 2004. The operation, dubbed "Titan Rain," resulted in the theft of terabytes of sensitive data, including export-controlled technology, though the DOD is understandably hesitant to describe the size and scope of the data loss. An analyst involved in the investigation asserted that the attackers left behind "backdoors," allowing them access at a later date; if true, this would permit future data collection as well as providing the access needed for a future malicious cyber-attack.[34]

Those with knowledge of the incident insist that the evidence indicates the Chinese government was responsible for the attack. However, as with most well-planned cyber-attacks, attribution is difficult. Without proper and provable attribution, it is difficult for a nation to respond to a cyber-attack. This example is valuable because it demonstrates the ease with which one nation can spy on another. Additionally, it enables espionage with little personal or political risk, since attribution is so challenging. Similar to the Titan Rain intrusion, in 2007, suspected Chinese individuals hacked F-35 subcontractor BAE Systems and made off with an unprecedented amount of data in an operation American officials refer to as Byzantine Hades.[35] Unsurprisingly, six years later, the People's Liberation Army Air Force debuted a suspiciously sophisticated stealth fighter prototype with F-35 characteristics.[36]

---

[33] Bradley Graham, "Hackers Attack Via Chinese Web Sites," *The Washington Post*, sec. Technology, 25 August 2005, http://www.washingtonpost.com/wp-dyn/content/article/2005/08/24/AR2005082402318.html (accessed 30 March 2014).

[34] Nathan Thornburgh, "Inside the Chinese Hack Attack," *Time*, 25 August 2005, http://content.time.com/time/nation/article/0,8599,1098371,00.html (accessed 11 April 2014).

[35] Sydney, J. Freedberg, Jr. "Top Official Admits F-35 Stealth Fighter Secrets Stolen," *Breaking Defense*, 20 June 2013, http://breakingdefense.com/2013/06/top-official-admits-f-35-stealth-fighter-secrets-stolen/ (accessed 11 Aril 2014).

[36] China's Global Times newspaper reported in January that China "completely obtained the six key technologies" from the F-35. A fire-control array radar system, thrust-vectoring jet nozzle, electro-

Cyber Policy and Organizations: USG Responses to Cyber-attacks

Large organizations, especially bureaucracies as large as governments, are particularly challenged by the threats posed via the cyber domain. Bureaucracies are culturally slow to change, and their size creates problems generating inertia to change; cyber operations, on the other hand, evolve quickly and can literally create effects at the speed of light.[37] Due to these reasons, governments typically find themselves in reactive postures rather than proactive postures when dealing with cyber threats. The following section describes the US policies and organizations created during the past two decades, often as a direct response to an attack via the cyber domain. As with the acts of espionage, sabotage, and profit-seeking described previously, understanding the evolution of US laws, policies, and new organizations will improve the reader's understanding of how and why the US Air Force forced organizational change beginning in 2006.

1986-87 – Early Policy. After increasingly common intrusions into government and corporate computers, the US Congress passed the Computer Fraud and Abuse Act (CFAA) of 1986, making it a crime to break into computer systems. Interestingly, the CFAA did not cover

---

optical targeting system and a diverterless supersonic inlet are among them. Staff, "China's New Fighter Made with Stolen F-35 Secrets," *Military1.com*, 14 March 2014, http://www.military1.com/defense/article/460449-chinas-new-fighter-made-with-stolen-f-35-secrets (accessed 17 March 2014).

[37] References to slow-moving bureaucracies are common; government bureaucracies are especially prone to excessive rigidity and come with following established routine. Two excellent books that discuss this bureaucracy and resultant problems are Gareth Morgan, *Images of Organization* (Thousand Oaks, CA: Sage Publications, 2006) and the *Model II* behavior described in Graham T. Allison and Philip Zelikow, *Essence of Decision: Explaining the Cuban Missile Crisis*, Second Edition (New York: Longman, 1999). That "cyber-attacks happen at the speed of light" has become a cliché. It is not technically true, since electrons traveling through connected networks experience resistance that light particles do not. However, cyber effects can be nearly immediate, especially when compared to the effects of traditional military, government, and criminal operations. Credible documents that refer to cyber effects traveling at light speed include: White House, *The National Strategy to Secure Cyberspace*, February 2003, xii, https://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf (accessed 14 April 2014) and Susan W. Brenner, "At Light Speed: Attribution and Response to Cybercrime/Terrorism/Warfare," *Journal of Criminal Law and Criminology*, Issue 2 Winter, Vol 97, Article 2, 379, http://scholarlycommons.law.northwestern.edu/cgi/viewcontent.cgi?article=7260&context=jclc (accessed 17 April 2014).

juveniles and it defined a "protected computer" as a computer (1) exclusively for the use of a financial institution of the USG or (2) which is used in or affecting interstate foreign commerce or communication.[38] The following year, President Ronald W. Reagan signed the Computer Security Act of 1987, a law designed to improve the security of sensitive information in federal computer systems. It required the creation of computer security plans and the appropriate clearance for the users of federal computer systems holding sensitive information.[39] Although this was one of the rare occasions in which major policy reform preceded, rather than resulted from, a major cyber event, the implementation of this law did not prevent Robert Morris's from releasing his worm into the ARPAnet. However, the USG successfully convicted Morris using the CFAA.

1988 – Computer Emergency Response Team. In 1988, as a response to the Morris Worm, the Computer Emergency Response Team (CERT) Coordination Center was created using funds from the DOD's Defense Advanced Research Project Agency (DARPA), the agency that developed the Internet's predecessor ARPAnet in the mid-1960s. The organization was designed to be a central reporting center for major internet security problems.[40] The CERT has grown into an academic-public-private partnership that includes the Software Engineering Institute at Carnegie Mellon University, law enforcement personnel, and the DHS.[41] CERT is the first organization developed in response to a cyber incident, and its staying power and diverse membership are indicators of its success. Unfortunately, despite the White House

[38] Title 18 U.S. Code § 1030, *Fraud and Related Activity in Connection with* Computers, http://www.law.cornell.edu/uscode/text/18/1030 (accessed 04 April 2014).
[39] Dan Rep Glickman, "H.R.145 - Computer Security Act of 1987," Legislation, January 6, 1987, http://thomas.loc.gov/cgi-bin/bdquery/z?d100:HR00145:@@@D&summ2=m& (accessed 18 March 2014).
[40] Staff, "Timeline: The U.S. Government and Cybersecurity," Washington Post, 16 May 2003.
[41] "About Us," United States Computer Emergency Readiness Team, undated, http://www.us-cert.gov/about-us (accessed 14 April 2014).

Assistant Director for National Security Affairs proclaiming that data theft "is a serious strategic threat to national security," CERT was the last meaningful organization created to combat cyber threats until the National Infrastructure Protection Center stood up in 1998. In fact, it was the last new major cyber policy action taken for nearly a decade, when the President's Commission on Critical Infrastructure Protection was established.

1996 – The President's Commission on Critical Infrastructure Protection. Following a July 1996 General Accounting Office (GAO) report stating that the DOD network experienced approximately 250,000 intrusions in 1995 – 65% of which were assessed as successful – President William J. Clinton established the President's Commission on Critical Infrastructure Protection (PCCIP), tasked "with coordinating and protecting vital infrastructure systems (gas, oil, telecom, water, transportation, etc.) against physical and electronic attack," though the focus was primarily on cyber threats.[42] Ultimately, the commission was expected to recommend a comprehensive national policy and implementation strategies.[43]

1997 – ELIGIBLE RECIEVER 97. In June 1997, the Joint Chiefs of Staff mandated the conduct of the first-ever No-Notice Interagency Exercise, to be titled *ELIGIBLE RECEIVER 97-1*.[44] The exercise was designed to test Department of Defense planning and crisis action capabilities while DOD information infrastructures were under attack. This large-scale exercise included all four armed services, most of the Geographical Combatant Commands, National Security Agency (NSA),

---

[42] Staff, "Timeline: The U.S. Government and Cybersecurity," Washington Post, 16 May 2003.
[43] Andrea Peterson and Sean Pool, "U.S. Cybersecurity Policy in Context," *Center for American Progress*, 22 February 2013, http://www.americanprogress.org/issues/technology/news/2013/02/22/54418/u-s-cybersecurity-policy-in-context/ (accessed 10 April 2014).
[44] Stephen W. Magnan, "Safeguarding Information Operations: Are We Our Own Worst Enemy?" Central Intelligence Agency, 14 April 2007, https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/summer00/art08.html (accessed 18 March 2014).

Defense Information Systems Agency (DISA), National Security Council (NSC), Defense Intelligence Agency (DIA), CIA, FBI, National Reconnaissance Office (NRO), and the Departments of State, Justice, and Transportation.[45] ELIGIBLE RECIEVER revealed significant and troubling vulnerabilities in USG information systems and deficiencies in responding to attacks on their information systems. According to the Congressional Research Office,

> The scenario was a rogue state rejecting direct military confrontation with the United States, while seeking to attack vulnerable U.S. information systems. Some of the goals of the rogue state were to conceal the identity of the attackers and to delay or deny any U.S. ability to respond militarily. A number of cyber-attacks (all simulated) were made against power and communications networks in Oahu, Los Angeles, Colorado Springs, St. Louis, Chicago, Detroit, Washington, DC, Fayetteville, and Tampa. Although reliable, unclassified results are hard to come by it is generally believed government and commercial sites were easily attacked and taken down. This exercise served as a wake-up call for many. Gen. Campbell, head of the Pentagon's Joint Task Force – Computer Network Defense, wrote Eligible Receiver "clearly demonstrated our lack of preparation for a coordinated cyber and physical attack on our critical military and civilian infrastructure." Then Pentagon spokesman Kenneth Bacon said, "Eligible Receiver was an important and revealing exercise that taught us that we must be better organized to deal with potential attacks against our computer systems and information infrastructure.[46]

United States Deputy Secretary of Defense John Hamre said of the exercise, we "know that [the Red Team was] very successful in penetrating DOD computers. I mean, we physically got messages from the bad guys on our own computers."[47] In the aftermath of the "Blue

---

[45] Staff, "Eligible Receiver," *Global Security*, undated, http://www.globalsecurity.org/military/ops/eligible-receiver.htm (accessed 10 April 2014).
[46] Steven A. Hildreth, "Cyberwarfare," *CRS Report for Congress*, 19 June 2001, http://www.fas.org/irp/crs/RL30735.pdf (accessed 11 April 2014).
[47] John Hamre, "Interview: Cyber War!" *PBS Frontline*, 24 April 2003, http://www.pbs.org/wgbh/pages/frontline/shows/cyberwar/interviews/hamre.html (accessed 08 April 2014); Notably, most contemporary descriptions of exercises of this type refer to them as

Team's" disturbingly poor performance during ELIGIBLE RECEIVER, the USG developed a flurry of new national policies to address the perceived weaknesses in the cyber domain.

1997 – Marsh Report Encourages Private-Government Cooperation. In October 1997, only months after ELIGIBLE RECEIVER, the President's Commission on Critical Infrastructure Protection released its first report, which highlighted the government's role in monitoring and disseminating new threat information to companies which rely on the cyber domain. The report is commonly referred to as "The Marsh Report" after PCCIP chairman Robert Marsh, a retired Air Force general and former Electronic Systems Division Systems Commander at Hanscom Air Force Base, Massachusetts. The commission's report cited no "evidence of an impending cyber-attack which could have a debilitating effect on the nation's critical infrastructures. While we see no electronic disaster around the corner, this is no basis for complacency. We did find widespread capability to exploit infrastructure vulnerabilities. The capability to do harm – particularly through information networks – is real. It is growing at an alarming rate; and we have little defense against it."[48]

The commission emphasized the need for action due to the rapid growth of a computer-literate population, the inherent vulnerabilities of computer networks, and the same easy availability of hacker tools that Michael Calce would describe as problematic nearly 15 years later. The commission recommended greater cooperation between private and public sectors, writing that "[T]he only sure path to protected infrastructures in the years ahead is through a real partnership

---

"information operations" exercises. In the 1990s, the USG terminology was still evolving; many aspects of what were then referred as "information operations" are now considered cyber-oriented in nature.

[48] General (ret) Robert T. Marsh, "Critical Foundations: Protecting America's Infrastructures," *The Report of the President's Commission on Critical Infrastructure Protection*, October 1997, 5, https://www.fas.org/sgp/library/pccip.pdf (accessed 03 April 2014).

between infrastructure owners and operators and the government. Because it may be impossible to determine the nature of a threat until after it has materialized, infrastructure owners and operators—most of whom are in the private sector—must focus on protecting themselves against the tools of disruption, while the government helps by collecting and disseminating the latest information about those tools and their employment."[49] Ultimately, the Marsh Report formalized what many high-level officials suspected: there is a threat due to relatively easily-learned hacker skills as well as the large number of unidentified vulnerabilities. Unfortunately, the report offered mostly generic recommendations rather than propose meaningful reforms that would offer improved security in the cyber domain. The creation of PCCIP was the first of a veritable wave of new policies and organizations created by the Clinton and Bush administrations in attempts to respond better to modern society's reliance on the cyber domain.

1998 – The FBI's National Infrastructure Protection Center and Presidential Decision Directive No. 63. The Marsh Report, the results of ELIGIBLE RECEIVER, and a February 1998 series of attacks on DOD unclassified networks dubbed *Solar Sunrise* led US Attorney General Jane Reno and FBI Director Louis Freeh to create the National Infrastructure Protection Center (NIPC). The center was charged with protecting all nationally critical infrastructure network systems for the government and private sector.[50] The agency was officially a part of the FBI, but it included elements from the Departments of Transportation, Energy, and Defense along with the National Security Agency (NSA) and the CIA. The center also forced closer coordination between the intelligence and security operations of the FBI and DOD. Additionally, since the most of the national infrastructure was owned by private

[49] Marsh, "Critical Foundations: Protecting America's Infrastructures," 5, x.
[50] "National Infrastructure Protection Center (NIPC)," http://ecommerce.hostip.info/pages/770/National-Infrastructure-Protection-Center-NIPC.html (accessed 10 April 2014).

corporations, those stakeholders were invited, forming a public-private governmental agency. The NIPC was transferred to the Department of Homeland Security in 2003, though its mission remained largely unchanged.

Shortly after the creation of the NIPC, President Clinton issued Presidential Decision Directive (PPD) Number 63. This implemented the National Infrastructure Assurance Plan, wherein groups were set up within the federal government to develop and implement plans to protect government-operated infrastructure. PPD63 called for a dialogue between government and the private sector to develop a National Infrastructure Assurance Plan to protect the national infrastructure no later than 2003.[51] The most notable aspect of PPD63 was that each federal agency was made responsible for securing its own critical infrastructure rather than charging a single agency with this important mission. This decision would lead to a wide variety of methods for securing USG cyberspace infrastructure, none of which were particularly effective. President Clinton attempted to provide oversight of this process by naming Richard Clarke as the National Coordinator for Security, Infrastructure Protection and Counterterrorism. President Clinton also requested a national cyberspace protection plan no later than 2000.[52]

The following year, in 1999, President Clinton released his National Plan for Information Systems Protection. This policy was solely focused on cybersecurity and advertised itself as a plan for "A Real Public-Private Partnership… Not Dictated Solutions."[53] Richard Clarke was responsible for the plan, and urged the redesign of our national information infrastructure architecture. Clarke remarked that,

---

[51] Peterson and Pool, "U.S. Cybersecurity Policy in Context," *Center for American Progress*, 22.
[52] Staff, "Timeline: The U.S. Government and Cybersecurity," *Washington Post*, 16 May 2003, http://www.washingtonpost.com/wp-dyn/articles/A50606-2002Jun26.html (accessed 10 April 2014).
[53] Clinton Administration, *National Plan for Information Systems Protection*, iv, http://clinton4.nara.gov/media/pdf/npisp-execsummary-000105.pdf (accessed 14 April 2014).

"[O]ver the last decade we built it quickly and without adequate concern for security, without thought that a sophisticated enemy might attack it. Now we must fix it, to protect, guard against, or reduce the existing vulnerabilities."[54] Unfortunately, as with PPD63, the National Plan for Information Systems Protection did not offer many details; rather it simply suggested a common framework for action by the USG and the private sector. The plan correctly identified improved education as a key to improving cyber security and emphasized that government systems should serve as the model for the private sector's infrastructure.

1999 – USG Increases Computer Security Budget. In January 1999, shortly after the USG's public acknowledgement of the MOONLIGHT MAZE intrusions, President Clinton announced a $1.5 billion initiative to improve government computer security. The plan established a network of intrusion detection monitors for certain federal agencies and encouraged the private sector to do the same. Notably, the $1.5 billion budget allocation marked a 40 percent increase over 1998 fiscal year spending and demonstrated the USG's willingness to devote resources to what was commonly considered a quickly growing security threat.[55] This figure grew to over $2 billion in fiscal year 2001, nearly double the 1998 budget.[56]

2000 – US Cybersecurity Strategy. In January 2000, the Clinton Administration released its cybersecurity strategy. The document was unpopular with private industry, which was inexplicably excluded from much of the drafting process. The strategy called for funding seven Public Key Infrastructure (PKI) pilot programs in FY 2001

---

[54] Clinton Administration, *National Plan for Information Systems Protection*, iv, http://clinton4.nara.gov/media/pdf/npisp-execsummary-000105.pdf (accessed 14 April 2014).
[55] John Christensen, "Bracing for Guerrilla Warfare in Cyberspace," *CNN Interactive*, 06 April 1999, http://cyber.law.harvard.edu/eon/ei/elabs/security/cyberterror.htm (accessed 04 April 2014).
[56] White House, "Protecting Cyber Security," undated, http://clinton5.nara.gov/WH/EOP/NSC/html/nsc-22.html (accessed 04 April 2014).

at different federal agencies; this was the basis for the Common Access Card (CAC) network login method common across the USG today.[57] The strategy also described a new "Federal Intrusion Detection Network to protect vital systems in federal civilian agencies, and to ensure the rapid implementation of system patches for known software defects."[58] Civil liberties and privacy groups opposed this, asserting it could dramatically expand government surveillance of the nation's communications networks. The administration quietly dropped its plans for an intrusion detection network.[59] This clearly demonstrates the challenge posed to governments of free societies: balancing the requirement to protect the people and the system without treading on the rights of those seeking protection.

2001 – The Post-9/11 Security Environment. Unhappy with President Clinton's national cybersecurity strategy and uncomfortable with the state of national security immediately after the 11 September 2001 terrorist attacks, President George W. Bush established the President's Critical Infrastructure Protection Board (PCIPB) and ordered the group to develop a national cybersecurity strategy in October 2001. Additionally, he moved Richard Clarke into a new role: White House Cybersecurity Adviser. The PCIPB immediately began soliciting advice from the private sector in order to avoid the criticisms levied at President Clinton's cybersecurity strategy. The PCIPB would publish the National Strategy to Secure Cyberspace in November 2002.[60]

President Bush also established the Office of Homeland Security and the Homeland Security Council by Executive Order (EO) in October

[57] White House, "President Clinton: Working to Strengthen Cybersecurity," undated, http://clinton4.nara.gov/textonly/WH/Work/021600.html (accessed 04 April 2014).
[58] White House, "President Clinton: Working to Strengthen Cybersecurity," undated, http://clinton4.nara.gov/textonly/WH/Work/021600.html (accessed 04 April 2014).
[59] Staff, "Timeline: The U.S. Government and Cybersecurity," *Washington Post*, 16 May 2003.
[60] Staff, "President's Critical Infrastructure Protection Board," *Federal Register*, undated, https://www.federalregister.gov/agencies/president-s-critical-infrastructure-protection-board (accessed 30 March 2014).

2001. The Office was charged with "protecting critical infrastructure from the consequences of terrorist attacks" and coordinating "efforts to respond to and promote recovery from terrorist threats or attacks within the United States" to include telecommunication. This EO made it clear which government organization was responsible for protecting the nation's critical IT infrastructure.[61]

2002 – National Strategy for Homeland Security. In mid-2002, the White House released the first *National Strategy for Homeland Security*. While its focus was on security against physical terrorist attacks, "Securing Cyberspace" was one of eight major initiatives identified in the document. The report also cited the upcoming *National Strategy to Secure Cyberspace* as one that "will describe our initiatives to secure our information systems against deliberate, malicious disruption."[62]

2003 – *The National Strategy to Secure Cyberspace.*
President Bush opened the National Strategy to Secure Cyberspace with this statement: "The way business is transacted, government operates, and national defense is conducted have changed. These activities now rely on an interdependent network of information technology infrastructures called cyberspace… The cornerstone of America's cyberspace security strategy is and will remain a public-private partnership."[63] After President Bush acknowledged that "securing cyberspace is an extraordinarily difficult strategic challenge," the *Strategy* outlined a framework for both organizing and prioritizing stakeholder efforts. It provided direction to the federal government that

[61] White House, "Executive Order 13228: Establishing the Office of Homeland Security and the Homeland Security Council," *Federation of American Scientists*, 08 October 2001, http://www.fas.org/irp/offdocs/eo/eo-13228.htm (accessed 10 April 2014).
[62] Office of Homeland Security, "National Strategy for Homeland Security," Department of Homeland Security, July 2002, 5, https://www.dhs.gov/sites/default/files/publications/nat-strat-hls-2002.pdf (accessed 10 April 2014).
[63] White House, *The National Strategy to Secure Cyberspace*, February 2003, 4, https://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf (accessed 14 April 2014).

had roles in cyberspace security and identified steps that state and local governments, private companies and organizations, and individual Americans should take to improve the nation's collective cybersecurity.[64] The *Strategy's* objectives included the prevention of cyber-attacks against America's critical infrastructure, reduction of national vulnerability to attack, and reduction of damage and recovery time from cyber-attacks that occur.[65] The document, as an implementing component to the *National Strategy for Homeland Security*, described national priorities for cyberspace security in an attempt to provide overarching framework to enable the public and private sector to combine efforts to improve America's cyber infrastructure. Unfortunately, many criticized this *Strategy* as "toothless" since it lacked regulations and other mechanisms to force internet service providers and hardware manufacturers to improve firewalls and security.[66]

2003-2005 – More Committees, Coordination, and Plans. In 2003, President Bush issued *Presidential Directive 7*, which provided a better definition of the relationship between the DHS and other agencies charged with cybersecurity. The Directive ordered that DHS maintain a cybersecurity unit while the Director of the Office of Management maintained responsibility for overseeing government-wide information security programs. The Director of Office of Management also operated the federal cyber incident response center within DHS. Additionally, the Directive created the Critical Infrastructure Protection Policy Coordinating Committee (CIPPCC), which advised the Homeland Security Council on interagency policy that related to physical and

[64] White House, *The National Strategy to Secure Cyberspace*, February 2003, viii.
[65] White House, *The National Strategy to Secure Cyberspace*, February 2003, viii.
[66] Robert Lemos, "Bush Unveils Final Cybersecurity Plan," *CNET,* 14 February 2003, http://news.cnet.com/2100-1001-984697.html (accessed 12 April 2014).

cyber infrastructure security.[67] President Bush's February 2005's Interim *National Infrastructure Protection Plan* (*NIPP*) aimed to provide "the framework and set the direction for implementing this coordinated, national effort."[68] Ultimately, both *Presidential Directive 7* and the Interim *NIPP* attempted to provide structure to an increasingly cluttered national security bureaucracy which had quickly filled with resource-seeking organizations in search of cybersecurity missions.

Military Missions, Organizations, and Policy: Evolving DOD Strategy

As demonstrated in the previous sections, illegal acts conducted via the cyber domain – to include for-profit crimes, criminal mischief, sabotage, and espionage – increased in frequency and severity from the early days of the ARPAnet to the early 21st century. In response to the increasing cyber threats to both private and government operations, the Clinton and Bush Administrations published increasingly frequent policy changes and created numerous organizations to protect American infrastructure. The Department of Defense shapes military policy based on the national strategy provided by civilian policymakers. However, in the case of cyber operations, the DOD in general and the USAF in particular, was impressively proactive.

1995 – USAF's *Foundations of Information Warfare.* In 1995, then-Secretary of the Air Force Shelia E. Widnall and then-Chief of Staff of the Air Force Ronald R. Fogleman jointly signed *The Foundations of Information Warfare.* This document laid the foundation for the USAF's approach to the cyber domain by providing definitions and principals for how the service would operate in cyberspace.[69] It made the critical

[67] "Homeland Security Presidential Directive 7," *Department of Homeland Security,* undated, http://www.dhs.gov/homeland-security-presidential-directive-7 (accessed 10 April 2014).
[68] "Interim National Infrastructure Protection Plan," *Department of Homeland Security*, February 2005, 1, http://net.educause.edu/ir/library/pdf/csd3754.pdf (accessed 10 April 2014).
[69] Jason Healey, "Claiming the Lost Cyber Heritage," *Strategic Studies Quarterly*, Fall 2012, 12. http://www.au.af.mil/au/ssq/2012/fall/fall12.pdf (accessed 02 February 2014).

first step in separating information warfare from cyber operations, though it never referred to the cyber domain. *The Foundations of Information Warfare* made a strict distinction between "warfare in the information age" and "information warfare." Warfare using computerized weapons such as a cruise missile is an example of the former, whereas "information warfare" treats information as an independent realm and a powerful weapon.

1996 – USAF Builds DOD's First Cyber Unit. In 1996, the Air Force created the DoD's first combat cyber unit more than a year before the DOD conducted the ELIGIBLE RECEIVER 97 exercise. The 609th Information Warfare Squadron (609 IWS) stood up at Shaw Air Force Base, South Carolina to support Air Forces Central (AFCENT), the air component to United States Central Command combatant command. Using combined offensive and defensive cyber capabilities, the unit's mission was "to fully operationalize information warfare on behalf of the JFACC [Joint Force Air Component Commander] and the fighting forces."[70] The 609 IWS demonstrated its capability immediately after its creation by taking control of the blue force air tasking order (ATO) within two hours, providing those involved with a preview of 1997 ELIGIBLE RECEIVER results.[71] However, even before the 609 IWS was created, the USAF had stood up other cyber units such as the Air Force Computer Emergency Response Team (AF-CERT, modeled after the CERT created at Carnegie Mellon in 1988) and the Air Force Information Warfare Center (AFIWC), but these units did not directly support the warfighter directly like the 609 IWS. AF-CERT, AFIWC, and

[70]Maj Gen (ret) John P. Casciano, assistant chief of staff, intelligence, United States Air Force (comments to Air Force Association National Symposia, 18 October 1996), http://secure.afa.org/aef/pub/la9.asp (accessed 02 February 2014).
[71] Atlantic Council event on 5 March 2012, "Lessons from Our Cyber Past: The First Military Cyber Units," http://www.atlanticcouncil.org/news/transcripts/transcript-lessons-from-our-cyber-past-the-first-military-cyber-units (accessed 02 February 2014).

609 IWS are the first cyber-focused organizations in the United States military, and are thought to be the first of their kind in the world.[72]

1997 – USAF Operationalizes and Professionalizes the Network. In 1997, Air Force leaders developed a new philosophy toward their networks and information systems. In January 1998, they formalized that philosophy and established a program titled Operationalizing and Professionalizing the Network (OPTN) in order to apply the same operational rigor toward USAF networks that the service used with weapons systems. OPTN established a hierarchical management system with operations centers at each Air Force base, subordinate to Major Commands, with the Air Force level residing at the top. OPTN also adopted the same operational reporting methods for Air Force network (AFNET) statuses and response measures as that of established weapons systems. Though OPTN was process-oriented, it addressed the key concerns USAF leadership had toward defending the AFNET from outside attacks.[73] USAF success in protecting service networks undoubtedly played a role when the SECDEF needed to select an officer to command the new joint service operations center to manage military networks.

1998 – An Airman as the First Joint Cyber Commander. The DOD recognized the importance of information networks and the cyber domain as critical infrastructure elements within the DOD after several events highlighted the vulnerabilities of defense networks. In December 1998, then-Secretary of Defense William S. Cohen appointed Air Force Major General John H. Campbell as Commander, Joint Task Force – Computer Network Defense (JTF-CND).[74] The SECDEF ordered the JTF to work with the unified commands, the military services, and other DOD agencies and charged Major General Campbell with ensuring the

[72] Atlantic Council, "Lessons from Our Cyber Past: The First Military Cyber Units."
[73] Scott D. Tobin, "Establishing a Cyber Warrior Force," *Air Force Institute of Technology Graduate Research Project*, September 2004, 15.
[74] Jason Healey, "Claiming the Lost Cyber Heritage," *Strategic Studies Quarterly*, Fall 2012, 12.

integrity and availability of DOD networks by "coordinating and directing the defense of DoD computer systems" from intruders and other attacks.[75] The JTF-CND reported directly through the Chairman of the Joint Chiefs of Staff to Secretary Cohen since the joint task force was not assigned to a unified command.[76] The Secretary increased the JTF's mission set in 2001 to include computer network attack and changed the unit's name to JTF for Computer Network Operations (JTF-CNO).[77] Maj Gen Campbell's selection as the first joint cyber commander demonstrated the policymakers' confidence in the Air Force's expertise in the emerging domain.

1999 – *Unrestricted Warfare.* In 1999, two Chinese People's Liberation Army Colonels wrote *Unrestricted Warfare*, a book on military strategy primarily providing options on how a nation such as China can defeat a technologically superior adversary such as the United States through a variety of means. The authors, Qiao Liang and Wang Xiangsui, argued that the US's primary weakness in military matters was that the United States military thought exclusively in terms of technology, that US military doctrine evolved because new technology allowed new capabilities. Because the American military is filled with technological determinists, Qiao and Wang insist, the US is vulnerable to other forms of attack as part of a wider military strategy.[78] Rather

---

[75] Robert J. Lamb, "Joint Task Force for Computer Network Defense," *IA Newsletter*, Winter 98/99, Vol 2, No. 3, http://www.iwar.org.uk/infocon/dtic-ia/Vol2_No3.pdf (accessed 10 April 2014).
[76] Press Release, "Joint Task Force on Computer Network Defense Now Operational," *U.S. Department of Defense*, 30 December 1998, http://www.defense.gov/Releases/Release.aspx?ReleaseID=1945 (accessed 14 April 2014).
[77] Clarence A. Robinson, Jr. "A Powerful Vision," *SIGNAL Magazine*, August 2001, http://www.afcea.org/content/?q=node/513 (accessed 14 April 2014).
[78] Neither of the two common translations of *Unrestricted Warfare* include the term "technological determinism." However, it is clear that, based on the context and how Qiao and Wang describe the American military, these officers feel the DOD is filled with technological determinists. This belief is consistent with the writings of many American authors, including Russell Frank Weigley, *The American Way of War: A History of United States Military Strategy and Policy*, Indiana University Press paperback ed, The Wars of the United States (Bloomington: Indiana University Press, 1977) and Merritt Roe Smith and Leo Marx, eds., *Does Technology Drive History?: The Dilemma of Technological Determinism* (Cambridge, Mass: MIT Press, 1994).

than focus on direct military confrontation, they instead examined asymmetrical ways and means such as applying international law ("lawfare"), economic warfare, and network warfare to circumvent the need for direct military action.[79] Qiao and Wang wrote, "[T]he new principles of war are no longer 'using armed force to compel the enemy to submit to one's will,' but rather are 'using all means, including armed force or nonarmed force, military and non-military, and lethal and non-lethal means to compel the enemy to accept one's interests.'"[80] With this passage, Qiao and Wang demonstrated a firm understanding that entering into a conventional conflict with the United States places an adversary at a decided disadvantage. After scrutinizing the elements of American military strength, the authors concluded that "the emergence of information technology has presented endless possibilities for match-ups involving old and new technologies and among new and advanced technologies."[81] Although these Chinese officers did not specifically promote targeting the US via the cyber domain, they did offer this: "[T]he damage of this type of [cyber] threat to the large network nation of the United States would certainly be greater than for other nations."[82] Qiao and Wang explicitly described asymmetric methods of successfully engaging a technologically superior foe that were very different from the asymmetric battles the United States faced in Vietnam, Iraq, and Afghanistan. The DOD barely understood this type of threat in the early 1990s; by the end of the decade, the Department conducted offensive and defensive cyber operations on a daily basis.

---

[79] David A. Adams, "Managing China's Transition," *Proceedings*. US Naval Institute, Annapolis: July 2003. Vol.129, Iss. 7, 50.
[80] Qiao Liang and Wang Xiangsui, *Unrestricted Warfare* (Beijing: PLA Literature and Arts Publishing House, February 1999), 7, http://www.c4i.org/unrestricted.pdf (accessed 28 March 2014).
[81] Qiao and Wang, *Unrestricted Warfare*, 4.
[82] Qiao and Wang, *Unrestricted Warfare*), 111-112.

2001-2003 – Cyberspace Defined. In April 2001, the Department of Defense's *Joint Publication 1-02, Dictionary of Military and Related Terms*, defined "cyberspace" as "the notional environment in which digitized information is communicated over computer networks."[83] Dr. Dan Kuehl from the National Defense University asserted, "[T]here was virtually universal agreement that [this definition] was insufficient: Cyberspace is hardly 'notional,' and confining it to 'digitized and computerized' is far too limiting, failing to reflect the massive technological and social changes with which cyberspace is interwoven."[84] The White House's 2003 *National Strategy to Secure Cyberspace* provided a critical improvement to this definition by defining cyberspace as the "nervous system—the control system of the country….composed of hundreds of thousands of interconnected computers, servers, routers, switches, and fiber optic cables that allow our critical infrastructures to work."[85] For the first time, cyberspace had a definition that approached the one we are familiar with today, though it was still unrecognized as a warfighting domain on par with land, sea, air, and space.

2001-2003 – NSPD-16, Operation IRAQI FREEDOM. Although many people remember Operations IRAQI FREEDOM (OIF) and ENDURING FREEDOM (OEF) as largely counterinsurgency operations, significant cyber operations occurred early both campaigns, particularly in OIF. First, during summer 2002, President George W. Bush signed National Security Presidential Directive (NSPD) 16, classified national guidance on the use of offensive cyber operations against adversary

---

[83] Joint Publication (JP) 1-02, *DOD Dictionary of Military and Related Terms*, dated 12 April 2001 and amended through 31 August 2005. www.dtic.mil (accessed 02 February 2014).
[84] Dr. Dan Kuehl. "From Cyberspace to Cyberpower: Defining the Problem.; Army War College. http://www.carlisle.army.mil/DIME/documents/Cyber Chapter Kuehl Final.doc (accessed 02 February 2014).
[85] United States Computer Emergency Readiness Team (Department of Homeland Security), *National Strategy to Secure Cyberspace,* February 2003. http://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf (accessed 02 February 2014).

nations.[86] As the United States-led coalition prepared for the March 2003 invasion of Iraq, unofficial reports indicated that cyber-attacks were planned in conjunction with traditional military operations.[87] During the opening days of OIF, the coalition cyber-attacks successfully deprived the Iraqi military and political leadership full use of their command, control, communication, and intelligence (C3I) network. The coalition air component attacked 116 communication and intelligence targets as part of what it called "information warfare physical attack."[88] Dr. Rebecca Grant, fellow at the USAF Ira Eaker Center, characterized these early operations:

> …[C]oalition forces were able to blend kinetic strategic attack with attacks in cyberspace. A primary target was the headquarters of the Republican Guard… General Moseley, the Air Force Chief, said at the time, "we started striking Republican Guards headquarters [at] minute one, and we never let up on them." The strikes, he added, "got us 48 to 72 hours ahead of anything they could do." As in previous wars, signals intercepts gave coalition commanders strong indications that the Iraqi military had broken down and descended into chaos… For all that, the net effect of the cyber assault in Iraq was to stoke fresh concerns about potential US vulnerabilities in the cyber domain. Commanders realized that sophisticated, real-time communications and data flow had become far more critical to US forces than it was for any potential foe. *US dominance of the battlespace hinged fatally on… the*

[86] Bradley Graham, "Bush Orders Guidelines for Cyber-Warfare: Rules for Attacking Enemy Computers Prepared as U.S. Weighs Iraq Options." *Washington Post*. 07 February 2003. This article is no longer available from the Washington Post website. However it is available at the following url: (http://www.stanford.edu/class/msande91si/www-spr04/readings/week5/bush_guidelines.html) and is referenced in articles at both CNN.com (http://www.cnn.com/2003/TECH/biztech/02/07/arms.cyber.reut/) and CBS.com (http://www.cbsnews.com/news/bush-wants-cyber-warfare-rules/).

[87] "Report: Bush Orders Guidelines for Cyber-Warfare," CNN, 07 February 2003. http://www.cnn.com/2003/TECH/biztech/02/07/arms.cyber.reut/ (accessed 02 February 2014).

[88] This was a wordy way to describe what were basically cyber operations that resulted in kinetic/physical results. "Operation Iraqi Freedom: By the Numbers," US Central Command Air Forces, 30 April 2003, 9, http://www.globalsecurity.org/military/library/report/2003/uscentaf_oif_report_30apr2003.pdf (accessed 02 February 2014).

> *dramatically large American edge in conventional warfare had now grown cyber-dependent.*[89] [emphasis added]

Dr. Grant's evidence comes directly from the Congressional Research Service: US military operations relied almost entirely upon a robust communications architecture, and the USAF was more dependent on this architecture than any other service. Processing, exploitation, and dissemination of national- and theater-level imagery placed an unprecedented burden on the network. Coalition forces during the opening months of OIF consumed bandwidth at a rate 30 times higher than the consumption during Operation DESERT STORM in 1991. The bandwidth used by Air Forces Central (AFCENT, the air component to US Central Command) increased nearly 600% the first day of combat. This made the Department of Defense the world's biggest bandwidth consumer.[90] The recognition that the US was uniquely vulnerable to cyber-attacks was disturbing, but change required partnership with the private sector; the recognition that America's armed serviced were uniquely vulnerable was the impetus for immediate change.

2004 – National Military Strategy. Lessons learned from the successful cyber operations in Iraq are subtly evident throughout the *National Military Strategy (NMS) of 2004*. This document asserted, "adversaries threaten the US throughout a complex battlespace," that includes "international airspace, waters, space and cyberspace."[91] The 2004 *NMS* concluded that "[t]he Armed Forces must have the ability to operate across the air, land, sea, space and cyberspace *domains* of the battlespace."[92] The Chairman of the Joint Chiefs of Staff, Air Force

---

[89] Dr. Rebecca Grant, "Victory in Cyberspace." 2007, 17-18, http://higherlogicdownload.s3.amazonaws.com/AFA/6379b747-7730-4f82-9b45-a1c80d6c8fdb/UploadedImages/Mitchell%20Publications/Victory%20in%20Cyberspace.pdf (accessed 02 February 2014).

[90] Clay Wilson, "Network Centric Warfare: Background and Oversight Issues for Congress," Congressional Research Service, Updated March 15, 2007 (accessed 02 February 2014).

[91] Department of Defense, *The National Military Strategy for the United States of America, 2004*, 5. http://www.defense.gov/news/mar2005/d20050318nms.pdf (accessed 02 February 2014).

[92] Department of Defense, *The National Military Strategy for the United States of America, 2004*, 8.

General Richard B. Myers, clearly considered cyberspace a domain on par with the natural domains, though no other joint document reflected this sentiment until DOD published the classified *National Military Strategy for Cyberspace Operations* in December 2006.[93]

Conclusion

In order to understand the significance of the USAF's decision to build a four-star cyber-focused headquarters, one must first understand the context of the national security environment in 2005. This chapter highlighted the rapidly evolving cyber threat by describing key cyber-attacks in recent history. Organizations began creating cyber effects more than 30 years ago. As time passed, networks were slowed and degraded, sensitive information stolen, and billions of dollars lost. The intentions for many attacks were clear: profit, mischief, espionage, sabotage. Additionally, the attackers were often clear and the acts attributable. However, for many attacks, the agent and the motive remain a mystery. This uncertainty, both in terms of attribution and motive, is a routine characteristic of cyber-attacks. This uncertainly provides some relief for the agents performing the attack while frustrating those suffering the attack. Finally, when the attacker and motive are unknown, it is difficult to hold guilty parties accountable for their actions, which makes cyber attacks an attractive opportunity for those with both capability and motive.

This chapter also explained the main USG policy changes and civilian organizations created to address the increased cyber threats in the two decades leading up to the Air Force decision to build a cyber-focused MAJCOM. Maintaining the required balance between security and privacy proved a challenge for civilian strategies and policies, but DOD strategies and policy were more aggressive in nature. Offensive

[93] Originally classified, this declassified document is now available publicly. http://www.dod.mil/pubs/foi/joint_staff/jointStaff_jointOperations/07-F-2105doc1.pdf (accessed 02 February 2014).

cyber capabilities were developed early by the Air Force, and forcing every DOD user to undergo training before logging on to machines with standard configurations improved DOD network security. However, the DOD recognized that both offensive and defensive cyber capability needed improvement in order to protect America's interests. This was the state of the national security in 2005.

Lastly, the evidence is unambiguous: the USAF was at the leading edge of cyberspace capabilities beginning in the 1990s and was the logical choice to continue this role as the DOD gradually grew to understand the importance of this domain to both military operations and national security. The USAF had more experience in the cyber domain than any other military in the world, and given the clear cyber threats to national security and USAF operations, the creation of a cyber-focused Air Force Major Command should have been anything but a surprise.

Chapter 3

Air Forces Cyber as a Major Command

In 2005, US Air Force leadership updated the service Mission Statement to include cyberspace as a warfighting domain, reflecting the 2004 *National Military Strategy* described in Chapter 2. Some accused the Air Force of "planting a flag in cyber" as a USAF mission while the other services were distracted with two resource-intensive land wars in Asia. In 2006, the USAF continued to stress the importance of the cyber domain to Air Force operations and national security. Secretary of the Air Force Michael W. Wynne created a Cyberspace Task Force to develop strategy and recommendations about how the USAF should approach cyber; the Task Force recommended a service Major Command to improve USAF ability to organize, train, and equip cyber forces to support warfighter requirements. The Air Force "thought leader in the cyber business," Lieutenant General Elder, was selected to create a service "on-ramp" to a cyber-focused Major Command.[1] Lt Gen Elder and his Eighth Air Force team worked tirelessly to build both an Air Force organization as well as an academic-industry-military collaborative relationship to leverage the field's best and brightest minds. Unfortunately, a series of embarrassing incidents led to a loss of confidence in the senior Air Force leadership. This resulted in a new Secretary, a new Chief of Staff, and new guidance on how the service would present cyber forces to the warfighting commanders.

This chapter describes decisions made by senior service leadership and the path traveled by the Air Force between 2005 and 2007. During these years, the most senior officer and civilian in the Air Force made decisions that some Department of Defense (DOD) senior leaders, sister service chiefs, and Air Force general officers found

[1] Lieutenant General William T. Lord, discussion with the author, 07 February 2014.

questionable; such as the choice to build a four-star Major Command focused on cyber operations. Despite some dissent, both vocal and silent, the USAF continued on its path of organizational transformation, forcing cultural change through education and training. When unrelated events interrupted this transformation, outside forces mandated different USAF organizational change. This chapter explains these organizational changes, competing internal and external forces, and the events leading to the USAF's organizational crisis.

2005 - Formalizing USAF's Relationship with Cyberspace

In December 2005, the newly-appointed Secretary of the Air Force (SECAF) Michael W. Wynne and then-Chief of Staff of the Air Force (CSAF) General T. Michael "Buzz" Moseley announced the service's new Mission Statement in a Letter to Airmen. It read, "The mission of the United States Air Force (USAF) is to deliver sovereign options for the defense of the United States of America and its global interests—to fly and fight in air, space, and *cyberspace*"[2] [emphasis added]. The difference between the previous Mission Statement and the new one was small, but noteworthy. The simple addition of cyberspace as a domain where the USAF would fight and defeat adversaries was a clear indicator of the significance of cyber operations to the most senior civilians and officers in the United States Air Force.

Lieutenant General Elder, Eighth Air Force Commander (8 AF/CC) and the officer General Moseley would eventually select to create an Air Force cyber headquarters, felt most people focused on the wrong part of the mission statement. In his view, the most important part of the new Mission Statement was the first half rather than the second half: that the mission of the USAF is to deliver *sovereign options*. Lt Gen Elder described how "sovereign options" was a term that

[2] Air Force Document (AFD) 111003-050, *Letter to the Airmen of the United States Air Force*, 07 December 2005, http://www.24af.af.mil/shared/media/document/AFD-111003-050.pdf (accessed 01 January 2014).

Secretary of Defense (SECDEF) Donald H. Rumsfeld often used with his staff. After the 11 September 2001 tragedy demonstrated the Department of Defense (DOD) was relatively unprepared for action across the range of military operations, Secretary Rumsfeld insisted that the military services provide him "sovereign options other than attrition warfare" that he could bring to the President of the United States. Secretary Wynne believed that cyberspace operations offered global effects, similar to those of long-range bombers, as an alternative to deploying troops or stationing maritime force off another country's coastline.[3] Ultimately, Secretary Wynne and General Moseley were surprised when senior Army, Navy, and Marine general and flag officers quietly criticized the USAF for trying to "claim cyber" as an Air Force mission when their intent was simply to comply with the SECDEF's expectations.

Secretary Wynne expressed sentiments similar to those offered in Chapter 2 when he wrote a Joint Letter to Airmen in 2005: namely, that the USAF is uniquely capable in the cyber domain. "[W]e have quite a few of our Airmen dedicated to cyberspace… from security awareness, making sure the networks can't be penetrated, as well as figuring out countermeasures. The Air Force is a natural leader in the cyber world and we thought it would be best to recognize that talent."[4] The Letter to Airmen also offered a more defined view of cyberspace: "[T]he term cyberspace includes network security, data transmission and the sharing of information." Secretary Wynne and General Moseley closed the Letter by writing, "If we can decisively and consistently control these commons, then we will deter countless conflicts."[5]

The decision to include cyberspace with air and space as a "commons" that must be kept free from the control of adversaries was a

[3] Lieutenant General Robert J. Elder, Jr., interview by the author, December 2013.
[4] Staff, "New Air Force Secretary Sends 'Letter to Airmen,'" *Air Force Space Command*, 04 November 2005, http://www.afspc.af.mil/news/story.asp?id=123026158 (accessed 12 April 2014).
[5] *Letter to the Airmen of the United States Air Force*, 07 December 2005.

bold statement by the SECAF and CSAF. Dr. Rebecca Grant, fellow at the USAF Ira Eaker Center, asserted that the USAF was simply "serving notice that it intended to operate freely in cyberspace. It was [as] real and important as any physical realm. The unmistakable corollary to this was that USAF would make a point of assuring US freedom of operation in all three domains."[6]

This Letter to Airmen and subsequent Mission Statement change were the first overt steps in a process that ultimately resulted in the creation of 24th Air Force (24 AF) as the operational headquarters responsible for organizing, training, and equipping cyber airmen while also presenting Air Force cyber forces to combatant and joint force commanders. The next step was to assemble a team of experts to offer courses of action to the CSAF.

2006 - QDR and the Cyberspace Task Force

The 2006 *Quadrennial Defense Review* (QDR) Report reinforced the USAF emphasis on the cyber domain, though it never applied that label. The report described terrorist abilities to "exploit the Internet as a cyber sanctuary" and advised "any attack on US territory, people critical infrastructure (including through cyberspace) or forces would result in an overwhelming response."[7] In the report, the DOD described concerns that China was "likely to continue making large investments in high-end, asymmetric military capabilities, emphasizing electronic and cyber-warfare," strikingly similar to Qiao and Wang's recommendations in *Unrestricted Warfare*.[8] The *QDR* Report also identified "capabilities to shape and defend cyberspace" as a military

[6] Dr. Rebecca Grant, "Victory in Cyberspace." 2007, 18, http://higherlogicdownload.s3.amazonaws.com/AFA/6379b747-7730-4f82-9b45-a1c80d6c8fdb/UploadedImages/Mitchell%20Publications/Victory%20in%20Cyberspace.pdf (accessed 02 February 2014).
[7] Department of Defense, *Report of the Quadrennial Defense Review*, 06 February 2006, 21 & 25, http://www.defense.gov/pubs/pdfs/qdr20060203.pdf (accessed 04 February 2014).
[8] Department of Defense, *Report of the Quadrennial Defense Review*, 06 February 2006, 58-59.

capability necessary to deter and win conflicts in the future.[9] The assessments made in the 2006 *QDR* Report represent a clear continuation of the strategic military documents described in Chapter 2: cyber threats were increasing and the DOD needed improved capabilities to defend the nation's security in cyberspace and shape cyberspace for friendly military operations.

In January 2006, the Secretary Wynne created the Cyberspace Task Force (CTF) to develop recommendations that included developing a USAF strategy for dominance across domains, evolving operational concepts for cyberspace and changing doctrine for these new missions.[10] Gen Moseley selected Dr. Lani Kass, a Professor of Military Strategy and Operations at the National War College and a Special Assistant to the CSAF, to lead his task force. Dr. Kass asserted that the United States Air Force was a uniquely technology-reliant organization. As such, the USAF was hyper-aware of potential cyberspace vulnerabilities and wished to repair or defend them. The need to address these issues led the USAF to commission the CTF, which included 10 Air Force officers, noncommissioned officers, and civilians with diverse backgrounds, including communications specialists, pilots, navigators, air battle managers, and intelligence personnel. Surprisingly, only one member of the CTF had true operational cyber experience. Even Dr. Kass, whose PhD was in Russian studies, lacked significant cyber experience.[11] Leveraging outside perspectives to develop solutions to strategic problems is both common and often successful.[12] Nonetheless, it is notable that a nominal team of experts

[9] Department of Defense, *Report of the Quadrennial Defense Review*, 06 February 2006, 32.
[10] Henry S. Kenyon, "Task Force Explores New Military Frontier," *SIGNAL Magazine*, October 2006, http://www.afcea.org/content/?q=node/1207 (accessed 08 February 2014).
[11] Colonel Forrest Hare, PhD, discussion with the author, 17 April 2014. Colonel Hare was a member of the CTF.
[12] This is a well-documented phenomena, and is at least partly attributable to the fact that outsiders are not constrained by the paradigmic beliefs like those within the "expert community." For more,

assembled to develop operational concepts for cyberspace included only a single individual that could speak knowledgably about the operational aspects of cyberspace.

One of the CTF's biggest challenges was to develop a common definition to communicate "what cyberspace means to the Air Force."[13] After nearly a year of research and hundreds of interviews, the task force concluded that cyberspace was a warfighting domain – military maneuver space – bounded by the electromagnetic spectrum. Dr. Kass noted the importance of harnessing the full range of Air Force capabilities by leveraging cyberspace throughout the service's terrestrial, airborne, and space networks. "By effectively integrating air, space and cyberspace, you create the ability to deliver targeted effects the way you choose anywhere, anytime. To sum it up in simple terms, cross-domain dominance equals *sovereign* operations," Dr. Kass told one interviewer [emphasis added].[14]

The CTF determined the USAF faced many challenges before it could meet its cyberspace goals. The largest obstacle required the service to transform itself to meet its current and future needs. Dr. Kass described this struggle: "It will be necessary to shatter existing paradigms entrenched in the purely kinetic traditions of warfare while transforming the force into a leader in cross-domain dominance of air, space and cyberspace. It's about the effects. Namely the effects we can produce in and through cyberspace upon our adversaries."[15] Dr. Kass also asserted that creating an Air Force command to focus exclusively on this issue would enable the service to respond to contemporary threats, think about tomorrow's conflict, and plan for 10-20 years into

---

read Thomas S. Kuhn, *The Structure of Scientific Revolutions*, Fourth edition (Chicago ; London: The University of Chicago Press, 2012).

[13] Henry S. Kenyon, "Task Force Explores New Military Frontier," *SIGNAL Magazine*, October 2006, http://www.afcea.org/content/?q=node/1207 (accessed 08 February 2014).

[14] Henry S. Kenyon, "Task Force Explores New Military Frontier," *Signal Online*. October 2006.

[15] Henry S. Kenyon, "Task Force Explores New Military Frontier," *Signal Online*. October 2006.

the future.[16] Dr. Kass's quote communicated her belief that the USAF required a culture change in order to fully leverage the cyberspace domain: she felt airmen's conceptions of airpower as simply offensive counterair, defensive counterair, and "bombs on target" were passé.[17] Instead, truly effective airpower required operations in air, space, and cyberspace. Although her views seemed somewhat heretical at the time, she was also convinced that only operators could fully operationalize the cyber domain: "The USAF approach to cyber was conceived and pushed forward by combat-experienced fighter pilots/WSOs—not [communications officers]."[18] She proudly believed that including individuals with an "enabler-mindset" would not help the USAF reach its goal.[19] Later decisions by senior Air Force leaders indicate that Dr. Kass's beliefs were popular on the Air Force staff.

The Cyberspace Task Force was only one team in the USAF performing research in this area; the Air Force's Research Laboratory (AFRL) was another. In 2006, Lieutenant Colonel Shane Courville from the Air War College's Center for Strategy and Technology interviewed

[16] Sgt Sara Wood, "New Air Force Command to Fight in Cyberspace," *US Department of Defense*, 03 November 2006 http://www.defense.gov/news/NewsArticle.aspx?ID=2014 (accessed 04 February 2014).

[17] Offensive counterair is "offensive operations to destroy, disrupt, or neutralize enemy aircraft, missiles, launch platforms, and their supporting structures and systems both before and after launch, and as close to their source as possible." Defensive counterair is "all defensive measures designed to neutralize or destroy enemy forces attempting to penetrate or attack through friendly airspace." *Joint Publication 1-02 Department of Defense Dictionary of Military and Associated Terms*, 08 November 2010. http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf (Accessed 13 April 2014).

[18] WSO is the USAF acronym, indicated Weapons Systems Operators. These are rated officers who have completed undergraduate navigation training and have been assigned to certain combat aircraft such as the F-15E and B-1. These "operators" are often held in higher regard than other navigators; Dr. Lani Kass, discussion with the author, 08 February 2014.

[19] In 2006, "communications" was categorized by the USAF as a "mission support" career field. Later, as part of Lt Gen Elder's program to operationalize cyberspace, communications airmen were dubbed "cyber airmen" and considered a "non-rated operations" career field, similar to intelligence airmen. In simple terms, Dr. Kass and USAF leadership felt that pilots and WSOs were better equipped to operationalize cyberspace than the airmen who dealt with cyberspace on a daily basis.

Dr. Kamal T. Jabbour, Principle Computer Engineer at the AFRL.[20] Dr. Jabbour assessed contemporary Air Force capability: "[W]e cannot see the attack coming. We have limited understanding of the threats. Attack attribution to the source is very difficult. Our only defense is within our boundaries. We have limited detection and prevention malware, combating an attack can result in the loss of mission capability and denial of service, and finally, [the] recovery process from an attack is done manually."[21] Between the CTF and AFRL, there appeared to be unanimity among the experts that the USAF needed to improve its cyber capability in order to protect national security interests and defend military operations.

The CTF briefed USAF senior leadership at the Fall 2006 CORONA Conference.[22] The discussions at these events are understandably close-hold, but one report indicated that the CTF offered two primary options on how the USAF should approach operations in the cyber domain: the service should create a new Numbered Air Force (NAF) or a new Major Command. The CTF preferred course of action was the a new MAJCOM.[23] However, many of the MAJCOM commanders in attendance favored the created of a cyber NAF rather than a cyber MAJCOM. Their reasons varied, but three arguments stood out from the rest. First, a component NAF is the organization through which the USAF traditionally (and doctrinally) presents forces to a warfighting commander. A component NAF "is structured to perform an operational and warfighting mission in support of a Unified Combatant

[20] Today, Dr. Jabbour is the Air Force's Senior Scientist for Information Assurance. http://www.af.mil/AboutUs/Biographies/Display/tabid/225/Article/108021/dr-kamal-t-jabbour.aspx (accessed 08 February 2014).

[21] Lt Col Shane P. Courville, "Air Force and the Cyberspace Mission: Defending the Air Force's Computer Network in the Future," Center for Strategy and Technology, Air War College, December 2007, 25. http://www.au.af.mil/au/awc/awcgate/cst/csat63.pdf (accessed 08 February 2014)

[22] CORONA Conferences are tri-annual summits, usually lasting approximately 3 days, designed to cover the breadth of issues facing the service. They are typically attended by the SECAF, CSAF, every 4-star Air Force general officer, and key 3-star Air Force general officers. Multiple officers present at this CORONA verified this version of events; all wished to remain anonymous.

[23] Colonel Hare, PhD, discussion with the author, 17 April 2014.

Command."[24] Component MAJCOMs, typically overseas MAJCOMs, were exceptions to this norm. In these cases, the MAJCOM acted as the USAF component to the theater's Geographical Combatant Command. For instance, Pacific Air Forces provided USAF component units for the United States Pacific Command while United States Air Forces in Europe provided component units for United States European Command.

Secondly, many of the commanders in attendance felt there was "not enough mission" for a cyber-focused MAJCOM.[25] This was a persuasive argument: Air Combat Command (ACC) owned nearly every fighter and bomber in the USAF inventory; Air Mobility Command owned nearly every airlift and air refueling asset; Air Education and Training Command was responsible for the recruiting, training, and education of all airmen. These commanders felt that there were not enough assets and resources to justify adding a cyber-focused MAJCOM to the USAF organizational structure.

This objection directly relates to the third and final objection. The creation of a new NAF would provide assets to an already existing MAJCOM; the creation of a *new MAJCOM*, on the other hand, would take resources away from the existing MAJCOMs. Unsurprisingly, no MAJCOM Commander was willing to surrender their assets and (potentially) part of their mission. Eighth Air Force (8 AF), for instance, was already conducting much of the mission the CTF described in their CORONA briefing. The Mighty Eighth owned a blend of electronic warfare assets, ISR assets, traditional combat assets, and network warfare assets. General Ronald E. Keys, ACC Commander, made a compelling case that the mission should simply go to, or remain with, 8 AF, which was one of his subordinate NAFs. Gen Keys insisted that by

[24] Air Force Doctrine Document 38-101, *Air Force Organization*, dated 16 March 2011, 19, http://static.e-publishing.af.mil/production/1/af_a1/publication/afi38-101/afi38-101.pdf (accessed 17 April 2014).
[25] General Norton A. Schwartz (ret), phone interview with the author, 07 February 2014.

giving the cyber mission to ACC, it could be better integrated with – rather than segregated from – combat assets.[26]

Ultimately, Secretary Wynne, after some discussion but little agreement among USAF senior leaders, elected to pursue a cyber-focused Major Command. General Moseley was noncommittal and deferred to the SECAF.[27] Secretary Wynne's decision was not altogether unexpected, since he sent the SECDEF a memo in January 2006 indicating the "AF has commenced planning for a Title 10 orientation to Organize, Train, and Equip… In the FY08 Budget, we will draw together the disparate elements which support this mission area as a part of the POM process."[28] Notably, this January 2006 memo was sent in the same month that the Cyberspace Task Force was formed, and nearly nine months before the CORONA where the issue was to be decided. Although this memorandum is not conclusive evidence that Secretary Wynne appointed the CTF to legitimize a decision that had already been made in January 2006, it is certainly suggestive.

2006 - Go-Do Letter and Developing an On-Ramp

Following the Fall 2006 CORONA Conference, Gen Moseley ordered Lt Gen Robert J. Elder, 8 AF/CC, to "develop an on ramp to transition" Eighth Air Force into a MAJCOM Component responsible for "the full spectrum of integrated global effects (kinetic and non-

[26] General Ronald E. Keys (ret), discussion with the author, 04 March 2014.
[27] A senior officer interviewed by the author indicated off the record that the SECAF permitted a short discussion, but it was clear that he favored the MAJCOM solution and would not be dissuaded by those in attendance. This senior officer also asserted that Secretary Wynne "wanted to make a statement that cyber rightly belonged to the Air Force."
[28] The Program Objective Memorandum (POM) is the primary document used by the Department of Defense (DOD), Army, and Navy to submit programming proposals. The POM includes an analysis of missions, objectives, alternative methods to accomplish objectives, and allocation of resources. USLegal Legal Definitions. http://definitions.uslegal.com/p/program-objective-memorandum-pom/ (accessed 15 April 2014); Secretary of the Air Force Michael W. Wynne to Secretary of Defense, memorandum, SUBJ: AF Cyberspace Efforts, 23 January 2006.

kinetic)."[29] General Moseley's vision for AFCYBER was lucid in this "Go Do" Letter, but the expectations from Lt Gen Elder were quite vague:

> This [order] reflects my intent to redefine air power by extending our global reach and global power into a new domain – the domain of electronics and the electromagnetic spectrum. The new mission of the MIGHTY EIGHTH will be to integrate the Air Force's global kinetic and non-kinetic strike capability in support of the combatant commander through the full range of military operations with authority to become COMAFFOR [Commander of Air Force Forces] for all USAF cyberspace elements… 8AF will provide the combatant commander with viable military operations through operational planning, integration, and execution in air, space and cyberspace… You will leverage, consolidate and integrate AF-unique cyber capabilities and functions – Command and Control, Electronic Warfare, Network Warfare, Surveillance and Reconnaissance, and Intelligence – across the spectrum of conflict, from peace to crisis to war…*you will organize your NAF around an Air Operations Center (AOC), able to operate 24 x 7 x 365, interoperable with all other AOCs* [emphasis added]… You will develop an "on ramp" to transition the MIGHTY EIGHTH into a MAJCOM Component responsible for presenting to and executing on behalf of COCOMs [sic] [combatant commands] the full spectrum of integrated global effects (kinetic and non-kinetic). Consider how you would enhance the AF presence at USSTRATCOM [United States Strategic Command] HQ in Omaha [Nebraska]… This is a bold move into a new warfighting domain, and I'm counting on you to lead us to dominance in this arena.[30]

The specific and direct order to organize the NAF around an Air and Space Operations Center (AOC) is noteworthy. It indicates that Gen Moseley intended AFCYBER's true focus to be on the operational level of war. This Air Operations Center, which would be a re-missioned 608th Air Operations Group (subordinate to 8 AF and already co-located with Eighth Air Force), would serve as AFCYBER's nucleus, the

[29] General T. Michael Moseley, Chief of Staff of the Air Force, to Lieutenant General Robert J. Elder, Jr., 8 AF/CC, memorandum, SUBJ: Operational Cyberspace Command "Go Do" Letter, 01 November 2006.

[30] Gen Moseley, to Lt Gen Elder, memorandum, SUBJ: Operational Cyberspace Command "Go Do" Letter.

place to consolidate and integrate both kinetic and non-kinetic effects in support of combatant commanders. Gen Moseley's order to Lt Gen Elder to prepare to be the "COMAFFOR for all USAF cyberspace elements" reinforced the operational focus of the future headquarters.

On the other hand, the memorandum was filled with buzzwords and expectations that the "AF dominate across…cyberspace" even though cyberspace dominance remained undefined and many felt that a lofty goal such as "cyberspace dominance" was impossible to achieve. Lt Gen Elder's planning staff, taken "out of hide" because Gen Moseley did not provide Lt Gen Elder an increased manpower authorization to complete this difficult task, struggled for months to "mission analyze" this letter, attempting to discern exactly was expected from Lt Gen Elder.

Historians that remember Eighth Air Force as World War II's "premier bomber Numbered Air Force" and contemporary airmen who only know Eighth Air Force as the USAF's "nuclear bomber Numbered Air Force" may consider the cyber mission set an odd fit for "The Mighty Eighth." However, as early as 2000, the USAF elected to integrate information operations into Eighth Air Force's organizational structure. In February 2001, the USAF realigned the Air Intelligence Agency (AIA) under Air Combat Command (Eighth Air Force's higher headquarters). The 67th Information Operations Wing and the 70th Intelligence Wing were then assigned to 8 AF, which already commanded the 2nd Bomb Wing (B-52), the 5th Bomb Wing (B-52), the 509th Bomb Wing (B-2), the 9th Reconnaissance Wing (U-2, RQ-4 Global Hawk, MC-12 Liberty), the 55th Wing (EC-130H electronic combat and RC-135 reconnaissance aircraft, and the 552nd Air Control Wing (E-3 AWACS). This 2001 reorganization transformed the "Mighty Eighth" into a truly integrated global-effects NAF that included bombers, reconnaissance aircraft, electronic combat aircraft, command and control aircraft, an intelligence wing, and the only information operations wing in the

service.[31] Eighth Air Force was uniquely equipped to execute any information operation needed by combatant commanders. In 2005, the primary discussion was whether cyberspace should be aligned with the communications community, the intelligence community, or the operational community. Once Gen Moseley decided that it belonged in operations, selecting the "Mighty Eighth" to lead the cyber charge was an obvious fit, just as General Keys proposed at the Fall 2006 CORONA Conference. Unlike Gen Keys's suggestion, however, the mission would not remain with Air Combat Command once Lt Gen Elder completed his project.

Another reason for the selection of Eighth Air Force to lead the development of the AFCYBER Major Command was the dual-hatted nature of the 8 AF/CC position. In July 2006, the Commander, US Strategic Command (CDRUSSTRATCOM) reorganized and identified Eighth Air Force as a sub-unified joint command subordinate to USSTRATCOM: Joint Functional Component Command for Global Strike and Integration (JFCC-GSI).[32] This meant that the 8 AF/CC would likely serve as CDRUSSTRATCOM's Joint Force Air Component Commander (JFACC) in times of conflict when USSTRATCOM was the supported command. Secretary Wynne and General Moseley deliberately selected the Air Force organization most suited to integrate information, cyber, and kinetic operations. They also selected the joint command, led by an airman, most able to follow the orders of the "Go Do" Letter: "Provide combatant commanders with viable military options… and execution in air, space, and cyberspace."[33]

---

[31] "Light from Darkness: A Short History of the 67 CW," 67th Cyberspace Wing, 4.

[32] History, United States Strategic Command, http://www.stratcom.mil/files/History.pdf (accessed 05 February 2014).

[33] Briefing. Lieutenant General Robert J. Elder Jr., 8 AF/CC, "Air Force Cyber Operations Command, Mission: Warfighting," 5 January 2007. http://www.au.af.mil/info-ops/usaf/cyber_ops_cmd_5jan07.pdf (Accessed 05 February 2014)

Lastly, Lieutenant General Elder was commonly thought to be the perfect candidate to lead USAF's operationalizing of the cyber domain. A rising USAF star, Lt Gen Elder earned his third star in only his 31st year of commissioned service.[34] The B-52 pilot earned a Doctor of Engineering Degree at the University of Detroit as a young Major. His diverse experience included tours as an F-15 Program Manager, a Global Positioning System (GPS) Program Officer, Chief of Strategic and Space Forces Branch, Assistant Director of Aerospace Operations, as well as commander as multiple levels.[35] Lt Gen Elder had the experience, the aptitude, and the charisma to meet the CSAF's goal.

General Moseley and Lt Gen Elder also had a great working relationship and similar ideas about promoting air power. Gen Moseley was the CSAF Chair at National War College (NWC) from 1989-1992, during which time Gen Elder was a NWC student.[36] Although they first met at NWC, the two officers did not work closely until 2001. In October 2001, Lt Gen Elder (then-Brigadier General Elder) moved to Shaw Air Force Base, South Carolina to become the Vice Commander of Ninth Air Force (9 AF/CV) and the Deputy Commander for Air Forces Central (AFCENT), the air component to United States Central Command (USCENTCOM). The following month, in November 2001, then-Lt Gen Moseley became the Commander of both 9 AF and AFCENT.[37] As General Moseley's deputy commander during the preparation for, and opening months of, Operation IRAQI FREEDOM, both officers had the opportunity to articulate and evolve their thoughts

[34] For perspective, Gen Keys – Lt Gen Elder's commander – took 33 years to earn his third star. Gen Moseley, the CSAF, earned his in 30 and one half years. Lt Gen Elder was charismatic, brilliant, and had an extremely bright future.

[35] Air Force Official Biography, Lieutenant General Robert J. Elder, Jr., http://www.af.mil/AboutUs/Biographies/Display/tabid/225/Article/104897/lieutenant-general-robert-j-bob-elder-jr.aspx (accessed 17 April 2014).

[36] Dr. Lani Kass was also a Strategy Professor at NWC at this time.

[37] Air Force Official Biography, General T. Michael Moseley, http://www.af.mil/AboutUs/Biographies/Display/tabid/225/Article/104651/general-t-michael-moseley.aspx (Accessed 05 February 2014); Air Force Official Biography, Lieutenant General Robert J. Elder, Jr.

on the proper role of the cyber domain in USAF and joint operations. Both witnessed the use of Air Force cyber capabilities in the early days of Operations ENDURING FREEDOM and IRAQI FREEDOM. They both departed Ninth Air Force in Fall 2003, and when then-Lt Gen Moseley was selected to be the Vice CSAF in 2004, he selected then-Maj Gen Elder to be the Commandant of the USAF Air War College (AWC) with the guidance to "put the war back in the War College."[38] While there, AWC students conducted several studies at Gen Moseley's request, including how to best integrate cyberspace with traditional USAF operations. It was at AWC that Lt Gen Elder first started working cyber issues with Dr. Kass, though he knew her well from his time as a student at NWC.[39] In June 2006, Lt Gen Elder was hand-selected by then-CSAF Gen Moseley to lead "The Mighty Eighth."

Simultaneously with Lt Gen Elder's assumption of 8 AF and JFCC-GSI, Major General John Maluda was selected to be Eighth Air Force's Vice Commander. Maj Gen Maluda was a career communications officer with 26 years of experience in satellite communications and C4ISR.[40] Having spent more than two years as ACC's Director of Communications (A6), Maj Gen Maluda – like Lt Gen Elder – was hand-selected for the difficult tasks that lie ahead. Interestingly, the selection of Maj Gen Maluda and his communications background as 8 AF/CV implied that he would also provide support to building the "on ramp" to the new cyber-focused MAJCOM. However, with both generals helping to build the CSAF's "on ramp" to a new MAJCOM, neither was able to focus exclusively on Eight Air Force's day-to-day operational mission. This may have played a role in the

[38] Lieutenant General Robert J. Elder, Jr., discussion with the author, 08 February 2014.
[39] Lieutenant General Robert J. Elder, Jr., discussion with the author, 08 February 2014.
[40] Air Force Official Biography, Major General John W. Maluda, http://www.af.mil/AboutUs/Biographies/Display/tabid/225/Article/104643/major-general-john-w-maluda.aspx (Accessed 05 February 2014); C4ISR is the USAF acronym for command, control, communications, computers, and Intelligence, surveillance, and reconnaissance.

2007 unauthorized nuclear transfer, though both Gen Keys and Lt Gen Elder insist that the transfer was an isolated event, unrelated to Lt Gen Elder's additional duties.

At the November 2006 C4ISR Integration Conference, Secretary Wynne stated, "My duty as the Secretary of the Air Force is to put the nation's most technologically capable force on a path to do our share of the task of presenting to our combatant commanders, and so to the President and the nation, the trained and ready forces they may need to ensure the same security and freedom of cyberspace that Americans and indeed many in the world already enjoy in the oceans, in the air, and also in space."[41] He stressed that the USAF was not attempting to gain control of cyberspace; instead, he intended to establish a "freedom of cyberspace [that] may in time be the same kind of principle as freedom of the seas and freedom of the skies."[42] Wynne cautioned that because the DOD is increasingly dependent on network- and computer-based systems, all other aspects of warfighting could be hindered without an increased focus on cyberspace. "This domain offers many unique opportunities and highlights a new inviolate principle: Without cyber-dominance, operations in all of the other domains are in fact placed at risk."[43] Wynne stated that the USAF planned to expand AFCYBER into a major command led by *a four-star general*, placing the new organization on equal footing with Air Combat Command and Air

[41] Michael W. Wynne, Secretary of the Unites States Air Force, "Cyberspace as a Domain in which the Air Force Flies and Fights" (address, C4ISR Integration Conference, Crystal City, VA, 02 November 2006) http://www.airforcemag.com/SiteCollectionDocuments/Reports/2006/November/Day03/Wynne110206.pdf (accessed 04 Februrary 2014).

[42] Wynne, "Cyberspace as a Domain in which the Air Force Flies and Fights"

[43] John T. Bennett, "Air Force to Establish New Cyberspace Operations Command," *World Politics Review*, 04 October 2006. http://www.worldpoliticsreview.com/articles/233/air-force-to-establish-new-cyberspace-operations-command (accessed 04 February 2014).

Force Space Command, which would give it the influence necessary to fight for service resources [emphasis added].[44]

This bold statement surprised many USAF senior leaders; no officers interviewed for this project expected the SECAF to make the statement, and none knew where this four-star billet would come from. Since general officer billets are regulated by US Code, a new position cannot simply be created.[45] Instead, it must be moved from one organization to another. This marked a large change for the AFCYBER plan. Up until now, participants expected Eighth Air Force to transition to a "Global Effects MAJCOM" that would integrate cyber operations with ISR, electronic warfare, and kinetic strike assets.[46] This organization would be led by a three-star general. Many expected Lt Gen Elder, for obvious reasons, to command this new organization by simply moving 8 AF out of Air Combat Command. At this point, that there was clear miscommunication within the USAF about what the final AFCYBER organization would look like.

2006 - Changing the Culture with the Organization

At a roundtable discussion, Lt Gen Elder articulated his concern that "an adversary that can go in and could take away our domination of cyberspace."[47] Since the USAF relies upon freedom of movement in the cyber domain in order to carry out many of its wartime tasks, he cautioned that that an adversary's success in cyberspace may mean "taking away the speed, range, and flexibility that we provide to the Joint Force Commander. For our own use, we absolutely have to have

[44] Josh Rogin, "Air Force To Create Cyber Command," *FCW: The Business of Federal Technology,* 13 November 2006. http://fcw.com/articles/2006/11/13/air-force-to-create-cyber-command.aspx (accessed 04 February 2014).
[45] Title 10 U.S. Code § 526, *Authorized Strength: General and Flag Officers on Active Duty*, available at http://www.law.cornell.edu/uscode/text/10/526 (accessed 18 April 2014).
[46] Lieutenant General Robert J. Elder, Jr., discussion with the author, 08 February 2014.
[47] Lieutenant General Robert J. Elder Jr., commander, Eighth Air Force, US Air Force (address, Defense Writers Group roundtable, 13 June, 2007).

domain control. If we can't communicate with the aircraft, if we can't communicate with the spacecraft, we can't do our mission."[48]

In response to this requirement to defend our own network, the USAF created the Air Force Network Operations Command (AFNETOPS) in August 2006. This unit was charged with ensuring the security and functionality of all Air Force cyber networks.[49] Prior to the standup of AFNETOPS, USAF network operations responsibilities were distributed among 10 Major Command Network Operations and Security Centers (NOSC), each of which enforced their own network and computer standards. AFNETOPS represented the USAF's attempt to unify command of all cyberspace operations under Lt Gen Elder. "The biggest benefit of standing up a command structure for Air Force network operation is that it unifies command of the Air Force computer network under one person, who serves as the Air Force component commander and presents network operations forces to [United States Strategic Command's sub-unified command] Joint Task Force-Global Network Operations," Lt Gen Elder told one interviewer.[50] "We always think about our expeditionary capability in terms of moving people and equipment any place in the world. You have to realize we can go to any part of the world and we can start doing operations immediately because we can stand up the communications, the command and control systems, situation awareness systems, that we need to be able to do that… When we talk about cyber defense, we're not just talking about trying to fit some kind of better virus protection on a computer. We're talking about protecting this ability to do these interdependent joint operations."[51]

---

[48] Lt Gen Elder (address, Defense Writers Group roundtable, 13 June, 2007).
[49] Dr. Rebecca Grant, "Victory in Cyberspace" 2007, 23.
[50] Capt. Carla Pampe, "Air Force Changes Network Operations Structure," *Air Force Print News*, 31 August, 2006.
[51] Lt Gen Elder (address, Defense Writers Group roundtable, 13 June, 2007).

As discussed previously, USAF senior leaders were concerned with the enabler mindset they felt was common in the communications field. For this reason, Dr. Kass ensured the dominant presence of "operators" on her CTF and Gen Moseley charged a bomber pilot with a diverse operational background to develop the new MAJCOM's "on ramp." This theme was apparent very early in Lt Gen Elder's construction project. In one oft-presented briefing, Lt Gen Elder explained the phases of improving the USAF's ability to operate in cyberspace. Figure 1 shows that Lt Gen Elder's top priority was to "Change culture from cyber as force enabler to warfighting force." Since this was listed as "Phase One" in the briefing he often presented when describing 8 AF's path, Lt Gen Elder obviously felt that changing the USAF culture was the critical first step of achieving the ultimate goal of transitioning "The Mighty Eighth" into AFCYBER. One of Lt Gen Elder's initiatives in this phase was to redesign the communications career field. The Air Force Specialty Code assigned to both officer and enlisted communications career fields was changed to indicate these personnel were now "operators."[52] Additionally, Air Education and Training Command adjusted the training program for the officer and enlisted career fields to include a greater focus on operations. Figure 2 shows Lt Gen Elder's road map for operationalizing the career cyber career fields. Figure 3 provides a snapshot of Lt Gen Elder's conclusions and demonstrates that his primary concern was overcoming cultural challenges.

[52] "1-series" Air Force Specialty Codes are assigned only to "ops career fields." These include 11 (pilot), 12 (navigator), 13 (space and missile forces), and 14 (intelligence). Communications officers were assigned a 1-series AFSC to demonstrate the importance of an operational mindset. Most communications personnel in 2006 were assigned to Mission Support Groups at USAF wings to provide computer and network support to base personnel. Despite the formal AFSC change in 2009, most communications personnel continue to serve in support functions assigned to USAF Mission Support Groups.

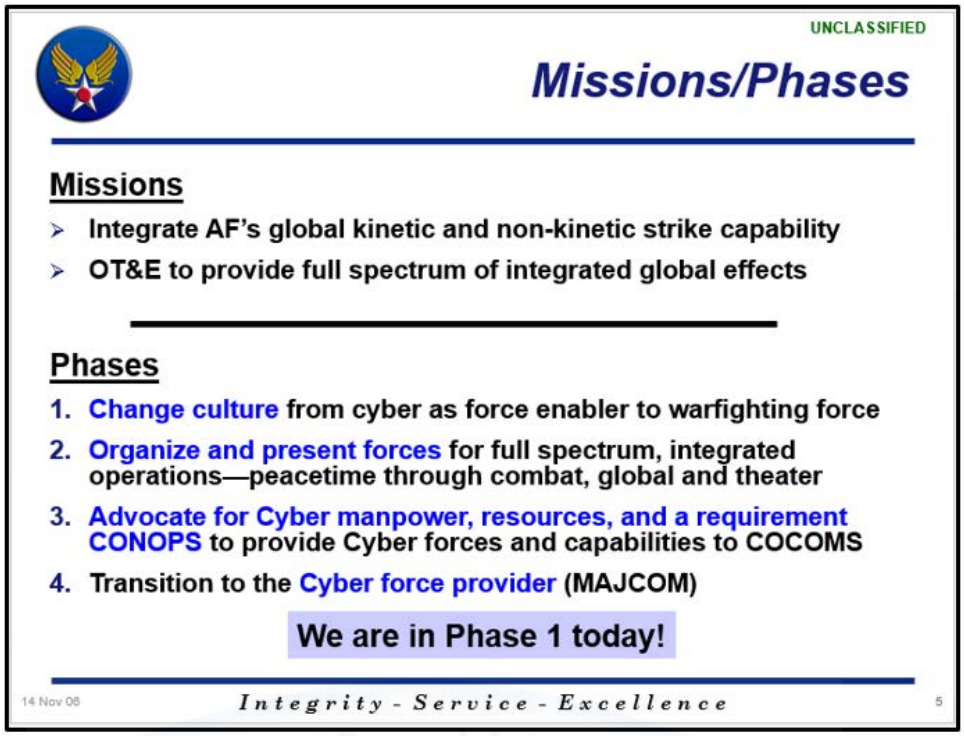

Figure 1. Lt Gen Elder's Priorities
8 AF Cybersummit Brief, 15 November 2006

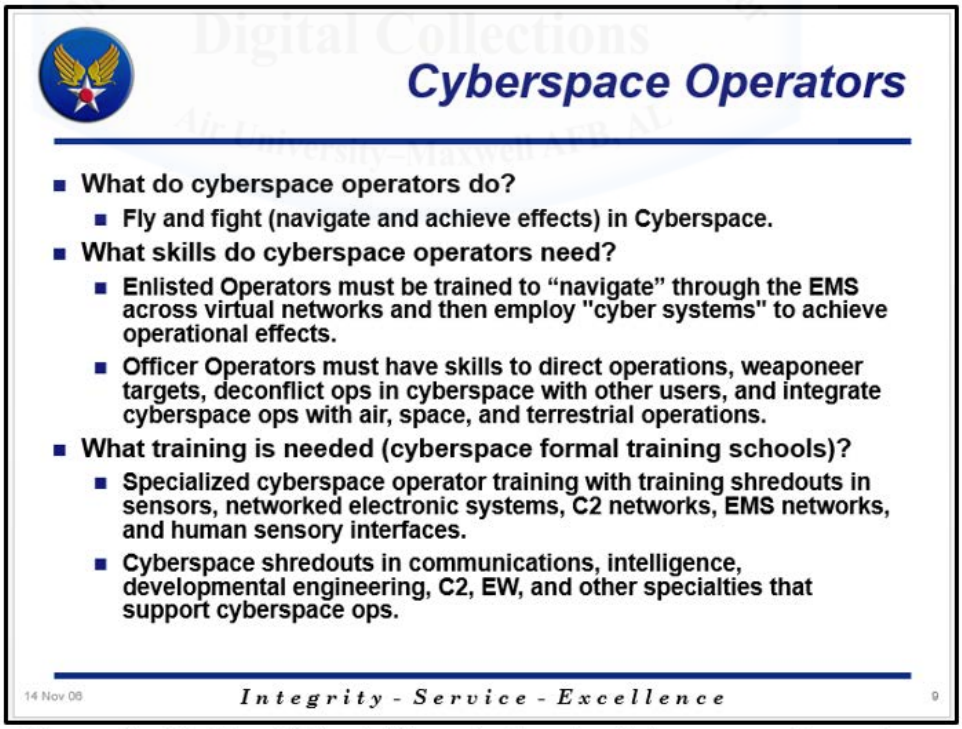

Figure 2. Lt Gen Elder's Plan to Create Cyberspace Operators
8 AF Cybersummit Brief, 15 November 2006

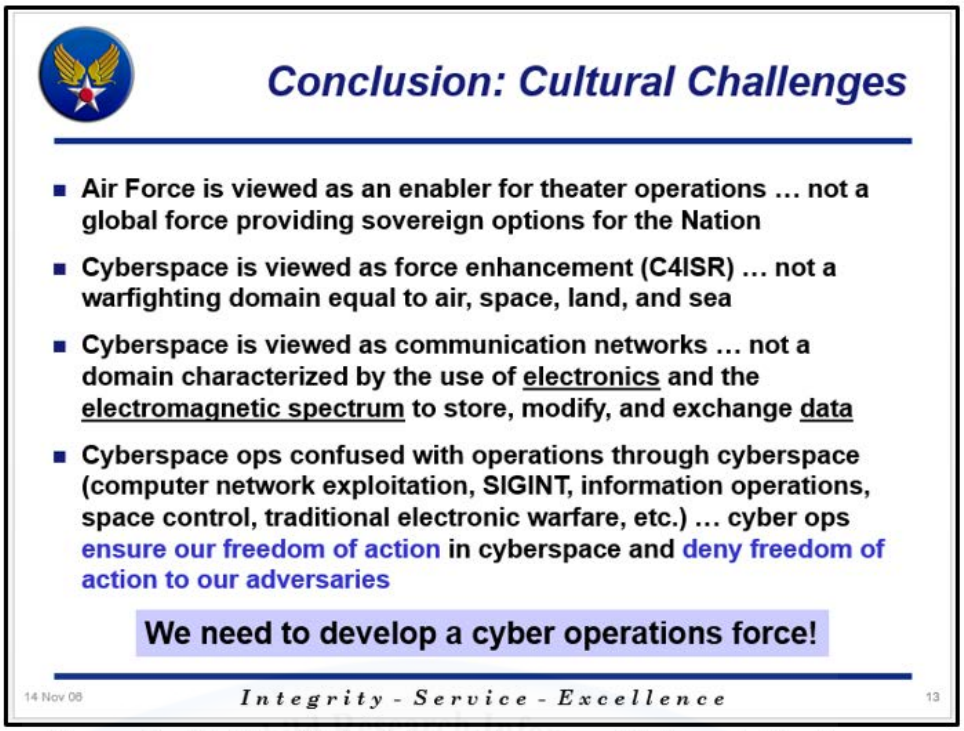

Figure 3. Lt Gen Elder's Top Concern: Cultural Challenges
8 AF Cybersummit Brief, 15 November 2006

2007 - Laying the Foundation in an Increasingly Dangerous Domain

With each passing month in 2007, it was increasingly evident that America's freedom of action in both space and cyberspace was far from certain. Global events demonstrated that the US should expect to be challenged in the two most recent additions to the DOD's list of warfighting domains, space and cyberspace. In January 2007, the People's Republic of China conducted its first successful direct-ascent anti-satellite (ASAT) weapons test, launching a ballistic missile to destroy a non-operable weather satellite at approximately 530 miles above Earth's surface in low earth orbit.[53] This confirmed China's program to develop weapons capable of targeting space assets—a program that put US military and intelligence satellites at risk. Given

[53] Shirley Kan, "China's Anti-Satellite Weapon Test," *CRS Report for Congress,* 23 April 2007, 2.http://www.fas.org/sgp/crs/row/RS22652.pdf (accessed 10 February 2014).

the fundamental relationship between the space and cyber domains, a threat in one domain poses a clear threat in the other.

Additionally, in April 2007, the Estonian government was the victim of a well-coordinated and widespread cyber attack that brought its technologically sophisticated government to a virtual standstill. As a result, Estonia, one of the world's most wired nations, was forced to completely sever international internet access.[54] As demonstrated in the previous chapter, this certainly was not the first cyber attack in history, but the Estonia attack proved that a cyber attack could effectively shut down this admittedly small nation. Cyber power was demonstrably a powerful coercive tool for those capable of wielding it.

Finally, insurgents in Afghanistan and Iraq easily exploited electronics and the electromagnetic spectrum via the use of improvised explosive devises. General Moseley pointed out in his 2007 White Paper that, "perhaps for the first time in the history of warfare, the ability to inflict damage and cause strategic dislocation is no longer directly proportional to capital investment, superior motivation and training, or technological prowess."[55] These events validated the USAF's position that the military services needed to change the way they considered the cyber domain. Perhaps as a result of these events, or as a result of the USAF venturing into the cyber domain, the US Navy and US Army began creating and improving cyber organizations within their services.

Throughout 2007, Lt Gen Elder presented frequent "roadshow" briefings to his bosses on Air Staff, to his peers and subordinate commanders, and at local universities and trade shows in attempts to provide updates and to recruit bright minds from academia and

---

[54]Gary Brown and Keira Poellet, "The Customary International Law of Cyberspace," *Strategic Studies Quarterly,*vol 6, no 3, Fall 2012, 130. http://www.au.af.mil/au/ssq/2012/fall/fall12.pdf (accessed 10 February 2014).

[55]General T. Michael Moseley, *The Nation's Guardians: America's 21st Century Air Force,* 5. http://www.au.af.mil/au/awc/awcgate/af/csaf_white_ppr_29dec07.pdf (accessed 10 February 2014).

industry to aid the process. Lt Gen Elder's *Partnership with Industry* was a successful effort that combined Air Force expertise with that of defense contractors to help both groups defend their networks.[56] This was an important campaign to build support for cyber operations not only within the service, but within academia and the private sector; a diverse and experienced group of individuals providing inputs would enable a broader perspective. This was considered critical since, at the time, the DOD was developing plans to help protect civilian networks as well. Additionally, a public demonstration of USAF's embrace of an emerging domain was expected to create excitement, both within the service and with the public. This drew many analogies to Billy Mitchell and the early days of air power.[57]

AFCYBER continued working toward Initial Operational Capability (IOC). After nearly a year of planning, Secretary Wynne ordered the activation of the Air Force Cyberspace Command (Provisional) (AFCYBER(P)) in September 2007, with the expectation that a permanent command would be activated no later than October 2008. Secretary Wynne and Gen Moseley selected Major General William T. Lord to command the provisional organization. Maj Gen Lord, like Maj Gen Maluda (8 AF/CV), was a career communications officer. In addition to this, he also commanded an Engineering and Installation Group and the 81st Training Wing, which is responsible for the education and training of every communications airman (both officer and enlisted). Additionally, prior to becoming AFCYBER(P)/CC, Maj Gen Lord served as the Director of Cyberspace Transformation on Air Staff in Washington, D.C. His experiences made him uniquely capable of developing and implementing plans for maturing cyber

[56] Lieutenant General Robert J. Elder, Jr., discussion with the author, 08 February 2014.

[57] Interestingly, Billy Mitchell's name came up multiple times while researching this thesis. First, at a public event in 2007, Secretary Wynne referred to Lt Gen Elder as "the Billy Mitchell of cyber." Lt Gen Elder was both surprised and embarrassed by this comment. Additionally, in a discussion with Dr. Kass, she referred to herself as "the Billy Mitchell of cyber."

operations as a USAF core competency. Additionally, he and Lt Gen Elder were close friends who had worked together as colonels on the ACC staff years earlier.

2007-2008 - Losing Confidence in USAF Leadership

Coincident with USAF's operationalization of cyberspace, the CSAF experienced steady friction when dealing with the Secretary of Defense, Robert M. Gates. The conflicts between the SECDEF and USAF senior leaders included criticism of two major acquisitions programs, the service's inability to rush more surveillance drones to support the efforts in Iraq and Afghanistan, and apparent conflicts of interest involving current and retired senior officials related to a $50 million Thunderbirds media contract.[58] However, the primary source of friction was with what Secretary Gates called "Next-War-itis" – "[T]he propensity of much of the defense establishment to be in favor of what might be needed in a future conflict… But in a world of finite knowledge and limited resources, where we have to make choices and set priorities, it makes sense to lean toward the most likely and lethal scenarios for our military… Overall, the kinds of capabilities we will most likely need in the years ahead will often resemble the kinds of capabilities we need today."[59]

For the Air Force, "Next-War-Itis" manifested itself in two related ways: spending service resources on hundreds of F-22 stealth fighters that Secretary Gates felt were unnecessary, and failing to provide more ISR (in the form of remote piloted aircraft, commonly referred to as "drones" or RPAs) to the war efforts in Afghanistan and Iraq. Critical of the military in general, and the USAF in particular, Gates was

[58] Staff, "U.S. Air Force Secretary, Chief Forced Out," *Defense News*, 05 June 2008, http://www.defensenews.com/print/article/20080605/C4ISR01/806050301/U-S-Air-Force-secretary-chief-forced-out (accessed 18 April 2014).
[59] Robert M. Gates, *Remarks to the Heritage Foundation*, U.S. Department of Defense, 13 May 2008, http://www.defense.gov/speeches/speech.aspx?speechid=1240 (accessed 18 April 2004).

incredulous that the services continued to spend money on high-technology equipment that had no place in most conflicts the US found itself in since WWII. For Secretary Gates, drones embodied the USAF's contribution to the new normal of irregular warfare, while Gen Moseley insisted 381 F-22s were an indispensable strategic hedge against future near-peer competitors. The Air Force could only think in terms of "high-tech air-to-air combat and strategic bombing against major nation states," Secretary Gates charged. He was frustrated that "every time Moseley and Air Force Secretary Mike Wynne came to see me, it was about a new bomber or more F-22s… [N]either would play any part in the wars we were already in."[60] In damning comments to the Air War College in April 2008, Secretary Gates exhorted, "My concern is that our services are still not moving aggressively in wartime to provide resources needed now on the battlefield. I've been wrestling for months to get more ISR assets into the theater. Because people were stuck in the old ways of doing business, it's been like pulling teeth."[61]

Despite this troubled relationship with the SECDEF, Secretary Wynne and Gen Moseley continued doing what they thought was best for the air service, including operationalizing the cyber domain. Nobody realized it at the time, but Secretary Wynne's and General Moseley's vision for how cyber airmen would support combatant and joint force commanders began to unravel at the end of August 2007, when a single event jeopardized the US Air Force's credibility more than any in recent memory. On 29 August 2007, a B-52 Stratofortress long-range bomber from the 5th Bomb Wing at Minot Air Force Base, North Dakota was scheduled to transfer six unarmed air-launched cruise missiles to

[60] John A. Tirpak, "Gates Versus the Air Force," *Air Force Magazine*, 05 February 2014, http://www.airforcemag.com/Features/Pages/2014/box020514gates.aspx (accessed 18 April 2014).
[61] Robert M. Gates, to Air War College students on 21 April 2008, as quoted by Jeff Donnithorne, "Tinted Blue: Air Force Culture and American Civil-Military Relations," *Strategic Studies Quarterly*, Winter 2010, 101, http://www.au.af.mil/au/ssq/2010/winter/donnithorne.pdf (accessed 18 April 2014).

Barksdale Air Force Base, Louisiana in order to be decommissioned, but munitions loaders inadvertently attached nuclear-armed missiles to the jet's pylons. The missiles were flown to Barksdale AFB and were left unguarded on the flightline for several hours before personnel noticed the mistake. In all, approximately 30 hours passed between the nuclear missiles upload at Minot AFB and their discovery at Barksdale AFB.[62]

These bomb wings were subordinate to 8 AF, complicating the Mighty Eighth's plans to build (or transition to) a cyber-focused MAJCOM. As the result of the nuclear transfer, a bomb wing commander, two group commanders, and two squadron commanders were relieved of their commands. Lt Gen Elder escaped reprimand for the failures of his bomb wings due to a skip-echelon agreement that absolved him of responsibility for the nuclear operations of these wings. After the event, Gen Moseley ordered a service-wide review of the USAF's nuclear enterprise. In May 2008, the results of the investigation were released, criticizing many deficiencies in the USAF's nuclear enterprise. When these findings were considered with a recent investigation into the USAF's 2006 mis-shipment of four nuclear warhead fuse assemblies to Taiwan, Secretary Gates concluded that problems with the USAF's nuclear weapons handling procedures were systemic rather than isolated.[63]

In June 2008, only three months before AFCYBER(P) was to become an operational headquarters, Secretary Gates requested the resignations of both Secretary Wynne and General Moseley. Secretary Gates elected to pursue this option after reviewing a May 2008 investigative report from US Navy Admiral Kirkland Donald, Director of Naval Nuclear Propulsion, which described a "gradual erosion of nuclear

[62] Staff Report, "Moseley and Wynne Forced Out," *The Air Force Times,* 05 June 2008. http://www.airforcetimes.com/article/20080605/NEWS/806050301/Moseley-Wynne-forced-out (accessed 10 Feb 2014).
[63] "Moseley and Wynne Forced Out," *The Air Force Times,* 05 June 2008.

standards and a lack of effective oversight by Air Force leadership."[64] Gates commented that the "overall mission focus of the Air Force has shifted away from this nuclear mission."[65] As the result of his loss of confidence in Air Force leadership, Secretary Gates requested letters of resignation from Secretary Wynne and General Moseley in June 2008. Both complied, and their departure led to a substantial change in how their vision for an operational cyber headquarters evolved.

Conclusion

Few expected the Air Force's path to a cyber-focused Major Command to be an easy journey, but nobody anticipated the problems the service experienced. This chapter described how Secretary of the Air Force Michael W. Wynne planned for an AFCYBER Major Command earlier than is publicly acknowledged. His memorandum to the SECDEF was dated before the Cyber Task Force ever met and months before the CORONA Conference where the MAJCOM-v-NAF debate was discussed by USAF senior leadership.

Secretary Wynne was forward-looking, but his urgency to demonstrate USAF capability in the cyber domain led to frustration, miscommunication, and confusion within the service. His decision to make the new organization a MAJCOM was unpopular with many 4-star general officers, but their objections were overruled with little explanation. These were the men responsible for leading airmen; although disenfranchising them did not have any obvious negative effects, their full support may have improved the odds of AFCYBER surviving in the form envision by Secretary Wynne. Secretary Wynne further confused matters when he asserted that the new cyber MAJCOM would be led by a four-star general so that it could better compete with the other similarly-ranked MAJCOMs for resources. This

[64] "Moseley and Wynne Forced Out," *The Air Force Times,* 05 June 2008.
[65] Robert Gates, Remarks to Pentagon Press Corps, 5 June 2008, http://www.defense.gov/transcripts/transcript.aspx?transcriptid=4236.

revelation surprised even insiders and posed a threat to the MAJCOM's current and future assets.

Despite the challenges, Lt Gen Elder and his Eighth Air Force staff performed yeoman's work. They spent more than 18 months building a plan and travelling across the country to brief that plan to leaders in military organizations, academics, and industry. While Eighth Air Force created partnerships across the country, they continued to chart a course for communications officers and airmen to become cyber operators in order to breed a mindset that senior leaders felt would make them more effective warfighters.

Unfortunately, while the nation fought two Asian land wars against non-technical enemies, and while Air Force leadership advocated the purchase of cutting-edge technology to ensure the US had no near-peer competitors, and while Eighth Air Force laid the foundation for a global effects MAJCOM, the service experienced a gradual erosion of its nuclear standards. This was a striking accusation, as the nuclear mission (in the form of strategic bombing) was the service's *raison d'être*. The nuclear exchange, and the USAF preference for high-tech gadgetry and resultant "Next-War-Itis," resulted in Secretary Wynne's and Gen Moseley's forced resignations. With this turnover at the most senior level of the Air Force, the service lost its most powerful advocates for an AFCYBER MAJCOM. Ironically, the same USAF culture that led airmen to grasp for the newest technology-dominated domain is the same culture that led to a too-narrow focus on high-tech acquisitions and poisoned the relationship between USAF and DOD leaders, resulting in an AFCYBER that bears little resemblance to the one envisioned by Secretary Wynne at the 2006 CORONA Conference.

Chapter 4

Air Forces Cyber as a Numbered Air Force

After years of professional disagreements, an independent determination that the service's nuclear standards had eroded due to a "lack of effective oversight by Air Force leadership" provided Secretary of Defense Robert M. Gates grounds to fire Secretary of the Air Force Michael W. Wynne and Chief of Staff of the Air Force General T. Michael Moseley. Their replacements had strikingly different views on how to run the Air Force, and these views had a profound effect on the future of the AFCYBER organization.

Secretary Gates selected General Norton A. Schwartz as the new Air Force Chief of Staff due largely to Gen Schwartz's vast joint experience. For Secretary Gates, this made Gen Schwartz more of an Air Force outsider than any other officer eligible for the Chief of Staff position. Gen Schwartz's fresh perspective led to many changes, not the least of which was the decision to downsize AFCYBER from a component Major Command to a Numbered Air Force. This was far from a simple decision, however.

This chapter describes the new direction for AFCYBER and examines the reasons for the change. Rather than a simple appeasement to the Secretary of Defense and the sitting Major Command commanders, there were several other variables in General Schwartz's decision calculus. Given the prescriptions offered in the *Report of the Secretary of Defense Task Force on Department of Defense Nuclear Weapons Management*, the new Secretary of the Air Force and Chief of Staff of the Air Force were faced with difficult decisions regarding missions, manpower, and personnel. Additionally, their style of leadership and vision for the cyber domain and cyber operations made them more receptive to viewpoints from outside their inner circle. This chapter also describes Lt Gen Elder's and Maj Gen

Lord's responses to this vector change, as well as the new path AFCYBER took on its way to reaching Full Operational Capability.

2008 – New USAF Leadership

Secretary of the Air Force (SECAF) Michael W. Wynne and Chief of Staff of the Air Force (CSAF) T. Michael Moseley submitted their retirement requests on Thursday 5 June 2008. Secretary of Defense (SECDEF) Robert M. Gates identified their replacements to Congress at the beginning of the following week, recommending Michael B. Donley as the new SECAF and General Norton A. Schwartz as the new CSAF.[1] The selection of Gen Schwartz provided insight into Secretary Gates's expectations from the USAF's senior leaders.

General Schwartz could not have been more different from General Moseley. Whereas Gen Moseley was outgoing and gregarious, Gen Schwartz was quiet and thoughtful. General Moseley was a fighter pilot, just like every Air Force Chief of Staff since 1982. General Schwartz was an airlift and special operations pilot, the first such CSAF in the service's history. Most importantly, however, General Schwartz had more joint experience than any active duty Air Force four-star general officer. General Schwartz had also worked exclusively in joint positions since January 2000. For Secretary Gates, this meant that Gen Schwartz was the least "institutionalized" USAF general officer eligible for the position; it also meant that he was likely more in tune with joint requirements, expectations, and relationships than most of his peers. This is the primary reason Secretary Gates selected Gen Schwartz to lead the Air Force.[2]

[1] Press Release No 486-08, "Defense Secretary Gates Announces Recommendations to the President on Senior Air Force Leadership Positions," *Defense.gov*, 09 June 2008, http://www.defense.gov/releases/release.aspx?releaseid=11975 (accessed 18 April 2014).

[2] This is by General Schwartz's own admission; he insists he was hired due to the fact that he was "the most joint four-star available." Although this might be a self-effacing exaggeration, the author chose to take him at his word.

In an open demonstration of support for Secretary Gates, Secretary Donley and General Schwartz publicly acknowledged that 183 F-22 fighters would be enough for the Air Force and that the Air Force would redouble efforts to increase ISR drones in Iraq and Afghanistan. Most importantly to this project, however, Secretary Gates and General Schwartz immediately issued a "stop order" in the operational standup of an AFCYBER Major Command (MAJCOM), halting all personnel assignments and the activation of units. General Schwartz and Secretary Donley insisted on a "comprehensive assessment of all AFCYBER requirements… to synchronize the AFCYBER mission with other key Air Force initiatives."[3] During remarks to the press, Secretary Donley implied that a cyber Major Command may not be the ideal decision and that the USAF's cyber command must "fit with US Strategic Command and the broader national security community."[4] The "stop order" and these public comments marked the first time that the USAF openly reconsidered the future of the service's cyber headquarters.

As discussed in the previous chapter, there were several motives for the "stop order." First, the USAF initiatives to consolidate all of its cyberspace units and budgets immediately generated antibodies both inside and outside the service, and this opposition was often based the fear of losing power, mission, or resources. Inside the service, four-star commanders, protective of "rice bowls," were hesitant to build a new organization that would compete with theirs for allocated assets and future budget dollars. Outside the service, opposition was based on similar concerns; specifically, that the USAF was attempting to become the executive agent (EA) for cyber as it had become for the space. An unintentionally inflammatory March 2007 memo from

[3] Staff, "On Pause, but Not Abandoning," *Air Force Magazine,* 14 August 2008. www.airforcemag.com/DRArchive/Pages/2008/August 2008/August 14 2008/OnPause,butNotAbandoning.aspx (accessed 12 February 2014).
[4] Staff, "On Pause, but Not Abandoning," *Air Force Magazine,* 14 August 2008.

General Moseley to Deputy Defense Secretary Gordon England, the Chairman of the Joint Chiefs of Staff, the service Chiefs, and every combatant commander compounded this concern. The memorandum proposed that the USAF take over as executive agent for all unmanned aerial vehicles (UAV) designed to operate at or above 3,500 feet, an idea that elicited an understandably toxic reaction among Army leadership. Army Brigadier General Stephen D. Mundt, director of aviation for the Army's deputy chief of staff for operations and plans, responded in an interview: "We absolutely disagree, and every other service does, too, and the Joint Staff does as well. Someone explain to me when a line in the sky became a service core competencies [sic]. My helicopters fly above 3,500 feet. That does not mean they belong to the Air Force."[5]

Another motive for the "stop order" was to give USAF's new leadership an opportunity to consider all available options and to consult with the Air Force experts. Both Secretary Donley and General Schwartz understood that many Air Force four-star general officers had opposed the cyber MAJCOM idea in 2006 and they remained opposed to it two years later. Stopping all action on the plan in August 2008 would allow open discussion at the CORONA Conference scheduled in October 2008.

During this hiatus, in September 2008, the Department of Defense (DOD) released the *Report of the Secretary of Defense Task Force on Department of Defense Nuclear Weapons Management*, a report ordered by the DOD in response to the recent USAF nuclear enterprise embarrassments. This report, commonly referred to as *The Schlesinger Report* because the chairman of the investigative commission was former Secretary of Defense James R. Schlesinger,

[5] Rebecca Grant, "The Drone War," *Air Force Magazine*, July 2007, Vol. 90, No. 7, http://www.airforcemag.com/MagazineArchive/Pages/2007/July%202007/0707drone.aspx (accessed 19 April 2014).

indicted the Air Force and the service leadership for their lack of focus on the service's nuclear mission:

> The Task Force found that there has been an unambiguous, dramatic, and unacceptable decline in the Air Force's commitment to perform the nuclear mission and, until very recently, little has been done to reverse it. Senior leadership decisions during the past 15 years have had the cumulative effect of compromising the Air Force's deterrent capabilities… The change in bomber mission focus away from a cadre of nuclear experienced personnel to conventional-warfare experienced Airmen was accompanied by a gradual decline in nuclear expertise, including in the senior leadership… Today no senior leader in the Air Force "owns" the nuclear mission. The current organization is not properly structured to meet requirements. Assigning a major Air Force command the responsibility for representing all Air Force nuclear-capable forces to U.S. Strategic Command (USSTRATCOM) will create nuclear mission alignment with that globally focused customer.[6]

Among other suggestions, the Schlesinger Commission recommended that all US Air Force bombers should be assigned to Eighth Air Force and that all non-bomber-related missions be removed from Eighth Air Force. The report specifically included the cyber mission as one which should be reallocated to a different Air Force MAJCOM.[7] This would allow the Eighth Air Force commander to focus exclusively on nuclear operations and "restore excellence to the nuclear deterrence mission."[8] The report made many suggestions, but this suggestion would serve as the impetus for considerable subsequent change.

In October 2008, a month after the release of the *Schlesinger Report*, Air Force senior leaders met at a CORONA Summit at Bolling

---

[6] Dr. James Schelsinger, "Report of the Secretary of Defense Task Force on DoD Nuclear Weapons Management, Phase I: The Air Force's Nuclear Mission," September 2008, 62. http://www.defense.gov/pubs/phase_i_report_sept_10.pdf (accessed 12 April 2014).
[7] *Schlesinger Report*, 62.
[8] *Schlesinger Report*, 51.

Air Force Base, Washington, D.C. At this conference, the Air Force's most senior general officers and civilians discussed the nuclear enterprise and the best way to organize USAF cyber forces, among other topics. Secretary Donley provided comments that indicated a strikingly different perspective from that of his predecessor: "The conduct of cyber operations is a complex issue, as DOD and other interagency partners have substantial equity in the cyber arena."[9] After the CORONA conference concluded, Secretary Donley's sentiment was confirmed. There had been a hearty debate and USAF senior leaders "collectively came to a decision" about the cyber and nuclear missions.[10]

2008 – AFCYBER Continues to Grow

Until General Schwartz issued the "stop order," Lieutenant General Robert J. Elder and Major General William T. Lord, 8 AF/CC and AFCYBER(P)/CC, respectively, continued their efforts to build AFCYBER into a global effects Major Command. Program Action Directive (PAD) 07-08 provided the specific guidance required to create the new command. PAD 07-08 directed that AFCYBER would be commanded by a Lieutenant General, despite Secretary Wynne's comments at the 2006 roundtable indicating otherwise.[11]

The new "global effects" MAJCOM would own two Numbered Air Forces (NAF). Eighth Air Force and all of its sub units, including 55th Wing, 9th Reconnaissance Wing, 432nd Wing, and the 480th Intelligence Wing would transition from Air Combat Command to

[9] Staff, "Air Force Senior Leaders Take Up Key Decisions," US Air Force, 07 October 2008. http://www.af.mil/news/story.asp?id=123118700 (original link), http://archive.is/BJrQ (archived link), accessed 12 February 2014.
[10] General Norton A. Schwartz (ret), phone interview with the author, 07 February 2014.
[11] Josh Rogin, "Air Force To Create Cyber Command," *FCW: The Business of Federal Technology,* 13 November 2006. http://fcw.com/articles/2006/11/13/air-force-to-create-cyber-command.aspx (accessed 04 February 2014); Headquarters United States Air Force, "Program Action Directive 07-08: Phase I of the Implementation of the Secretary of the Air Force Direction to Organize Air force Cyberspace Forces," 21 December 2007.

AFCYBER. Additionally, AFCYBER would also command a new ISR-focused NAF, to include the Air Force ISR Agency (AFISRA) and its sub units.[12] Once AFCYBER reached Initial Operational Capability, it would become the lead MAJCOM for USAF cyber operations, to include network operations, expeditionary and in-garrison communications, and installation services. Upon reaching Full Operational Capability, AFCYBER would transition to the global effects command Secretary Wynne envisioned; the MAJCOM would assume "lead MAJCOM responsibility" for global strike, global ISR, global C2, data integration, global operations integration, information operations, electro-magnetic spectrum operations, and Distributed Common Ground Systems (intelligence).[13]

Critically, when AFCYBER Provisional (AFCYBER(P)) was created in October 2007, manpower was allocated to build the new command. In other words, when Major General Lord arrived at Barksdale AFB, LA to help Lt Gen Elder build the "on ramp," he brought empty billets with him. Soon afterward, staff officers began to arrive, giving Lt Gen Elder's action officers an opportunity to return to their assigned, rather than additional, duties. Of course, these assigned duties were often still related to the new MAJCOM, since 8 AF would be subordinate to the new command. Additionally, the 608th Air Operations Group needed to transition to an Air and Space Operations Center (AOC), as directed in General Moseley's 2006 "Go Do Letter." Ultimately, despite the uncertainties about the new unit, the Mighty Eighth continued building AFCYBER until the new CSAF directed it to stop all actions in August 2008.

[12] PAD 07-08, 21 December 2007, 11-12.
[13] PAD 07-08, 21 December 2007, 16.

2008 - New Vector: 2-Star Cyber NAF, 3-Star Nuclear MAJCOM

At the 2008 CORONA Summit, in accordance with *Schlesinger Report* recommendations, Air Force senior leaders decided to establish a nuclear-focused Major Command to concentrate USAF support for the nuclear and deterrence missions. This coincided with General Schwartz's announcement that "strengthening and reinvigorating the nuclear enterprise" was the service's number one priority.[14] Shortly afterward, USAF leaders announced the creation of a new Major Command whose sole focus would be the Air Force nuclear enterprise. Air Force Global Strike Command (AFGSC) would organize, train, and equip all USAF nuclear forces, and 8 AF would become its subordinate NAF in charge of nuclear-capable bombers. Furthermore, consistent with Dr. Schlesinger's Task Force recommendations, all non-bomber-related missions were reassigned away from Eighth Air Force. The Mighty Eighth was, once again, the Air Force's foremost "Bomber NAF."

Additionally, USAF leadership chose to establish a NAF for cyber operations within Air Force Space Command (AFSPC).[15] Afterward, Secretary Donley and General Schwartz announced the Twenty-Fourth Air Force (24 AF) would gain the cyber warfare mission as part of AFSPC. They charged 24 AF with the mission to "extend, operate and defend the Air Force portion of the Department of Defense network and provide full spectrum capabilities for the Joint warfighter in, through and from cyberspace."[16]

---

[14] General Norton A. Schwartz, "The CSAF's Perspective," 13 August 2008, http://www.slideshare.net/steeljawscribe/csafs-perspective (accessed 20 April 2014); and Air Force Nuclear Task Force, "Reinvigorating the Air Force Nuclear Enterprise," Headquarters Air Force, 24 October 2008, http://www.fas.org/irp/doddir/usaf/nuclear.pdf (accessed 20 April 2014).

[15] Staff, "Air Force Senior Leaders Take Up Key Decisions," US Air Force, 07 October 2008. http://www.af.mil/news/story.asp?id=123118700 (original link), http://archive.is/BJrQ (archived link), (accessed 12 February 2014).

[16] 24th AF Public Affairs, "24th Air Force Fact Sheet," 03 January, 2013. http://www.24af.af.mil/library/factsheets/factsheet.asp?id=15663 (accessed 12 February 2014).

Although some reported that the decisions to create these two commands were unrelated to one another, the timing and structure of the organizations makes that seem unbelievable.[17] First, PAD 07-08 clearly indicates that Eighth Air Force was expected to move to the AFCYBER MAJCOM with most of its assets intact. The creation of AFGSC stripped Eighth Air Force of most of its assets – all but two B-52 wings and a B-2 wing – and assigned it under the new nuclear MAJCOM. Secondly, it would have been extremely difficult for the USAF to simultaneously create two new Major Commands, even if a Lieutenant General led them both; there are simply not enough excess 3-star generals available for such a plan. Lastly, Twentieth Air Force (20 AF, the nuclear missile NAF with three subordinate missile wings), was moved from Air Force Space Command (AFSPC) to AFGSC as part of the plan to centralize command of all of the service's nuclear units. This left only Fourteenth Air Force (14 AF) subordinate to AFSPC. It would be impossible to justify having a four-star general officer command a MAJCOM with only a single NAF as a subordinate. It made sense from a manpower and personnel perspective to assign 24 AF, the new AFCYBER Numbered Air Force, to Air Force Space Command so the mission would continue to merit a four-star MAJCOM commander. Additionally, General Schwartz felt that aligning the cyber mission under the established Air Force Space Command was a fundamentally sound decision from a functional perspective: both were "engineering intensive and space relied heavily on cyber."[18]

In May 2009, General Schwartz and Secretary Donley announced that Lackland Air Force Base, Texas would host the new 24 AF headquarters, and the Provisional Command began reassigning

[17] Rebecca Grant, "The Cyber Menace," *Air Force Magazine,* March 2009, Vol. 92, No. 3, http://www.airforcemag.com/MagazineArchive/Pages/2009/March%202009/0309cyber.aspx (accessed 19 April 2014).
[18] General Norton A. Schwartz (ret), interview with the author, 07 February 2014.

billets, bodies, and equipment to Lackland AFB almost immediately.[19] A month later, the USAF announced that Major General Richard E. Webber, a career missile officer with experience in both communications and space operations, was selected to be the first 24 AF commander.[20] During that spring, the USAF strengthened its cyber network by "announcing that maintenance tasking orders, network tasking orders, and cyber control orders had the same binding force as lawful general orders and aircraft maintenance time compliance technical orders."[21] This was an initiative by General Schwartz to foster a cultural change in the Air Force regarding cyber operations, similar to Lt Gen Elder's top priority in the development AFCYBER. As the Air Force Chief of Staff noted, Airmen "must treat our computers and networks similarly to our aircraft, satellites, and missiles."[22]

May 2009 also saw the release of Secretary Donley's and General Schwartz's first *United States Air Force Posture Statement* since assuming the service's top positions. For the first time, "Cyberspace Superiority" was listed as one of the USAF's core functions:

> Operating within the cyber domain has become an increasingly critical requirement for our networked force. In order to develop and institutionalize cyberspace capabilities, and to better integrate them into the Joint cyberspace structure, we are consolidating many Air Force cyberspace operations into a new 24th Air Force under Air Force Space Command. The Air Force is firmly committed to developing the necessary capabilities to defend the cyber

[19]Honorable Michael B. Donley, Secretary of the Air Force, to AFSPC/CC, et al., memorandum, 07 November 2009, "Final Basing Decision and Activation of 24th Air Force."
[20]Air Force Official Biography, Major General Richard E. Webber, http://www.af.mil/AboutUs/Biographies/Display/tabid/225/Article/105106/major-general-richard-e-webber.aspx (Accessed 16 February 2014).
[21] Dr. Gregory W. Ball, "24th Air Force Heritage Pamphlet: A Brief History of the Twenty-Fourth Air Force," 15 October 2012, 5. http://www.24af.af.mil/shared/media/document/AFD-121219-034.pdf (accessed 05 February 2014).
[22] Dr. Ball, "24th Air Force Heritage Pamphlet: A Brief History of the Twenty-Fourth Air Force," 5.

> domain, and our FY10 budget proposal includes $2.3B to grow this important Core Function.[23]

On 18 August 2009, the nascent cyber organization met all organizational and administrative requirements and General C. Robert Kehler, Commander of Air Force Space Command, presided over 24 AF's activation ceremony at Lackland AFB. During his comments, Gen Kehler remarked the unit's mission was "to integrate cyberspace operations with those in air and space to support military operations across the spectrum of conflicts… Adding 24 AF to the AFSPC team culminates a 2-year Air Force effort to centralize cyber capabilities in support of the joint warfighter and to adapt an operational perspective for this domain."[24] This new Numbered Air Force officially became the higher headquarters for the 67th Network Warfare Wing, the 689th Combat Communications Wing, the 624th Operations Center (assuming the mission and responsibility of the 608th Air Force Network Operations Center), and the 688th Information Operations Wing (previously the Air Force Information Operations Center).[25] Major General Webber's remarks at the ceremony reinforced the purpose of the new command to the audience:

> Today is truly an historic day for our Air Force. The activation of Twenty-Fourth Air Force continues the evolution of the Air Force's commitment to "Fly, Fight, and Win in Air, Space, and Cyberspace." We moved our cyber capabilities under Air Force Space Command as our lead command, continuing the evolution of cyber as a potent war fighting capability. Twenty-Fourth Air Force further demonstrates the Air Force's commitment to supporting Department of Defense objectives in cyberspace. *For the*

[23] United States Air Force Posture Statement, 2009, 19 May 2009, http://www.posturestatement.af.mil/shared/media/document/AFD-090522-062.pdf (accessed 18 April 2014).

[24] General C. Robert Kehler, "24th Air Force Activation," *Air Force Space Command,* 19 August 2009. www.24af.af.mil/news/story.asp?id=123163965 (accessed 16 February 2014).

[25] Staff, "24th Air Force Activated and Two Units Realign in Joint Ceremony," *Air Force Space Command*, 18 August 2009. http://www.afspc.af.mil/news1/story.asp?id=123163827 (accessed 16 February 2014).

> *first time in the history of the Air Force, we have consolidated cyber capabilities under an operational war fighter solely devoted to cyber operations.*[26] [emphasis added]

Secretary Donley and General Schwartz published a *Memorandum to all Airmen* on 20 August 2009. The letter outlined every step the USAF took to organize its cyber forces in the best way to present them to combatant commanders and joint force Commanders, then concluded with the statement that this organization marked the beginning of a process rather than the end.[27] He continued to stress the importance of airmen changing their mindsets: "[W]e must also change the way we think about the cyberspace domain, and accordingly change our culture. Like air and space, we must think of cyberspace as a mission-critical domain where operations are characterized by rigor and discipline, and are executed with precision and reliability… We must establish close and continuing relationships with our joint partners, industry, and academia… We will, in short, deliver on our promise to fly, fight and win… in air, space and cyberspace."[28]

Upon 24 AF's activation, the Secretary and CSAF designated Air Force Space Command as the lead USAF Major Command for the cyberspace mission. Additionally, they began the process to have 24 AF recognized as the Air Force service component to US Cyber Command (USCYBERCOM), aligning authorities and responsibilities to enable seamless cyberspace operations. With this move, 24 AF officially became "AFCYBER."[29]

---

[26] Dr. Ball, "24th Air Force Heritage Pamphlet: A Brief History of the Twenty-Fourth Air Force," 6.
[27] Dr. Ball, "24th Air Force Heritage Pamphlet: A Brief History of the Twenty-Fourth Air Force," 6.
[28] Honorable Michael B. Donley, Secretary of the Air Force and General Norton A. Schwartz, Chief of Staff of the Air Force, Memorandum to All Airmen, August 2009, "Air Force Cyberspace Mission Alignment."
[29] Donley and Schwartz, Memo to All Airmen, Aug 2009, "Air Force Cyberspace Mission Alignment."

Conclusion

Secretary Donley and General Schwartz took over a service in disarray; this was not the first time a SECAF or CSAF were dismissed, but it marked the first time in the service's history that both USAF senior leaders were dismissed simultaneously. Recent Air Force decisions had been unpopular in the DOD, with the sister services, and even within the service. Military services certainly are not expected to "play nicely together" all the time; in fact, competitiveness is an important element in the defense establishment. However, the DOD's displeasure with the USAF and her apparent commitment to service culture over the joint fight ended with the Air Force in the metaphorical penalty box. General Schwartz was hired to help the service overcome its propensity for new toys and improve joint relationships.

General Schwartz had messes to clean up within the service in addition to mending joint relationships. The unauthorized nuclear transfer and the subsequent commission that identified a "gradual erosion of nuclear standards and a lack of effective oversight by Air Force leadership" caused ripples so large that they impacted the creation of AFCYBER.[30] AFCYBER as a Major Command was an unpopular idea with the most senior USAF general officers. Even the new Chief of Staff of the Air Force admitted that he wondered if the 2006 decision to build a cyber MAJCOM was premature; he doubted the "USAF was ready to back up its rhetoric and make the required investments in terms of resources and human capital." Simply, General Schwartz felt that the original ambition of cyber may have been unrealistic and too aggressive.[31] Despite these feelings, he chose to consult his fellow four-star peers before making a quick decision on

[30] Staff Report, "Moseley and Wynne Forced Out," *The Air Force Times,* 05 June 2008. http://www.airforcetimes.com/article/20080605/NEWS/806050301/Moseley-Wynne-forced-out (accessed 08 Feb 2014)

[31] General Norton A. Schwartz (ret), interview with the author, 07 February 2014.

the AFCYBER Major Command. After debating the issue at the October 2008 CORONA Summit, Air Force senior leaders "collectively came to the conclusion that a Numbered Air Force under AFSPC was the best fit."[32]

The new organization took longer to create than intended, its mission is not as broad as originally envisioned, and the headquarters is not located where early planners expected. Although the path was more challenging than anyone anticipated, combining space and cyber assets, both offensive and defensive, within the same command created significant synergy: both can create global effects, kinetic and non-kinetic; both are technologically challenging and are often misunderstood by those unfamiliar with the threats and capabilities associated with each; and both are capable of presenting options to joint commanders around the clock without requiring a physical deployment of forces. Ultimately, although AFCYBER is very different than the organization envisioned by Secretary Wynne in 2005, it is exactly what the service leaders envisioned in 2008. External changes in the form of DOD perceptions of the USAF and internal changes in the form of a new SECAF and CSAF with a new vision and leadership styles, led to the institutional bargain that resulted in 24 AF.

[32] General Norton A. Schwartz (ret), interview with the author, 07 February 2014.

Chapter 5

Conclusions and Implications

This final chapter provides the conclusions and insights drawn from Lieutenant General Elder's and AFCYBER's unexpectedly long journey. Nine years after the new USAF Mission Statement, chaos and misunderstanding continue to reign in the cyber domain. The service is uncertain of its ability to guarantee freedom of movement and action in cyberspace, let alone its ability to gain and maintain cyberspace superiority. This is equally due to technological, legal, and policy challenges.

Additionally, this chapter demonstrates that the decision to organize Air Force cyber forces into a Numbered Air Force subordinate to Air Force Space Command was not the result of a calculated plan that was best for the service, or the nation, in the cyber domain. Rather, it was the result of organizational bargaining due to practical limits placed on the USAF's options on how to organize for the cyber mission. These limits include individuals and organizations protective of their missions and resources. Another limit was the USAF's new nuclear Major Command, which effectively ended AFCYBER's advocates' aspirations to become a Major Command.

Some assert that the results of these bargains have resulted in a watered-down USAF cyber capability. However, this limited capability is more due to the lack of cyberspace theory, uncertain lines between legal and military roles in cyberspace, and ambiguous strategic direction for military use of the domain. Ultimately, there is little evidence that a "global effects" Major Command would solve these problems any more effectively than 24 AF in coordination with the Department of Defense's other cyber agencies.

A Note about Author Bias

Before continuing with summary and assessments, I must confess two author biases. First, I assumed the Chief of Staff (CSAF) General T. Michael Moseley was the driving force behind the changed USAF Mission Statement and the plan to build an AFCYBER Major Command (MAJCOM). This assumption was likely based on the fact that I, as a uniformed servicemember, am more familiar with the face, name, role and responsibilities of the CSAF than of the Secretary of the Air Force (SECAF). During the course of my research, I determined that Secretary Michael W. Wynne rather than General Moseley acted as the agent of change. Secretary Wynne conceived the Mission Statement change and wanted an AFCYBER MAJCOM established quickly with a 4-star commander. Gen Moseley was agreeable to the proposition, and worked with Lieutenant General Robert J. Elder to operationalize the domain. Nearly every interviewee with knowledge agreed on these points.

Secondly, before conducting my research, I expected to "discover" that this was the story of a USAF power grab for the cyber domain. This is likely due to my understanding of intense service rivalries as described by Carl Builder, James R. Locher, and Owen Reid Cote, Jr.[1] Having read *Revolt of the Admirals* and *A Fiery Peace In A Cold War* in the last year, both of which described USAF insistence on claiming a particular mission as something the Air Force should exclusively perform, I had preconceived notions about what I would find during the course of my research.[2] In reality, however, I found little evidence of a service "power grab." Instead, Secretary Wynne and Gen Moseley both seemed to

[1] For more, please read Carl H. Builder, *The Masks of War: American Military Styles in Strategy and Analysis* (Baltimore: Johns Hopkins University Press, 1989); Carl H. Builder, *The Icarus Syndrom* (New Brunswick: Transaction Publishers, 1994); James R. Locher, *Victory on the Potomac the Goldwater-Nichols Act Unifies the Pentagon* (College Station: Texas A & M University Press, 2002); and Owen Reid Cote, Jr. "Politics of Innovative Military Doctrine: U.S. Navy and Fleet Ballistic Missiles," MIT PhD Dissertation, 1996.

[2] Jeffrey G Barlow, *Revolt of the Admirals: The Fight for Naval Aviation, 1945-1950* (Washington: Naval Historical Center, Dept. of the Navy : For sale by the U.S. G.P.O., Supt. of Docs., 1994); Neil Sheehan, *A Fiery Peace in a Cold War: Bernard Schriever and the Ultimate Weapon* (New York: Random House, 2009).

understand the threats and capabilities offered by the cyber domain, and elected to improve Air Force expertise in a *cyber*space domain that was a critical element in the USAF's ability to maintain freedom of movement in the *physical* (air and space) domains.

Observations and Analysis

Air Forces Cyber is now fully functional, but it is still trying to link its role with other USAF missions. This is not an indictment of the command, its subordinate wings, or the service to which it belongs. Rather, it is clear that the DOD's concept of operationalizing the cyber domain has not experienced the hoped-for success. According to all primary and secondary sources, 24 AF has performed as expected, but today's AFCYBER is certainly not as capable as the AFCYBER imagined in 2006. Secretary Wynne and General Moseley wanted the USAF to take the cyber lead, informally if not formally. However, while the Air Force has continued to perform well in the domain offensively and defensively, the recent appointment of a sailor to command the joint sub-unified US Cyber Command (USCYBERCOM) is an explicit sign that the Air Force model for cyber may not be the best one.

The US Navy took a remarkably different approach to the cyber domain than the USAF. Rather than attempting to operationalize it by placing "an operator" in charge (pilot/navigator in the USAF, Surface Warfare Officer in the USN), the Navy elected to merge their communications career fields with their intelligence career fields. Given the exploitation and targeting experience available in the intelligence career field, and the utility of that expertise to cyber operations, this seemed a natural fit. Indeed, the merging of the career fields and the synergy created played a large role in the selection of Admiral Michael S. Rogers as CDRUSCYBERCOM, a position which is dual-hatted with the Director of the National Security Agency (DIRNSA).

This, of course, raises the question of whether the USAF was wrong in its attempts to operationalize the cyber domain. This is beyond the scope of this project, but I urge interested readers to explore Carl H Builder's *The Icarus Syndrome*. The USAF's focus on airplanes and the men and women who fly them are certainly understandable, given the service's history. However, the USAF in 1950 had orders of magnitudes more planes and fewer mission sets than today's Air Force; contemporary service leaders' continued insistence that wearing wings makes one capable of not only commanding any type of unit, but operationalizing that unit, seems trite. The DIRNSA is now a sailor for the first time in nearly 20 years. USCYBERCOM was created in June 2009; its first commander was a soldier, and its second commander is a sailor.[3] If the opinions of the President of the United States, the SECDEF, and the Chairman of the Joint Chiefs of Staff can be considered a measurement of success, it appears that the Navy cyber model is a more successful one than that of the Air Force.

Nearly a decade after the USAF Mission Statement change, there is no consensus on the use of cyberspace. It is clearly critical to military operations; however, like diplomacy and economics, cyber has a large role in domestic and international politics. For this reason, many feel that cyber may be better classified as the "informational" instrument of national power rather than solely a military tool.[4] This is certainly an intriguing thought, and one that merits further exploration.

---

[3] U.S. Cyber Command Factsheet, U.S. Strategic Command, http://www.stratcom.mil/factsheets/2/Cyber_Command/ (accessed 20 April 2014).

[4] There are many examples. Here are but a few: Robert Kozloski, "The Information Domain as an Element of National Power," *Strategic Insights,* Center for Contemporary Conflict, Homeland Security Digital Library, 21 January 2009, http://www.hsdl.org/?view&did=232244 (accessed 20 April 2014); Robert Kozloski, "The Future of Military Force: Non-Lethal Force Could Be the Future of Warfare," Real Clear Defense, 24 February 2014, http://www.realcleardefense.com/articles/2014/02/24/the_future_of_military_force_107102.html (accessed 20 April 2014); Colonel Jayson M. Spade, "Information as Power: China's Cyber Power and America's National Security," U.S. Army War College, May 2012, http://www.carlisle.army.mil/dime/documents/China's%20Cyber%20Power%20and%20America's%20National%20Security%20Web%20Version.pdf (accessed 20 April 2014).

Ultimately, although society has become increasingly reliant on the cyber domain, its ubiquitous nature crosses the up-until-now clear line between civilian-military operations. The United States Government (USG) cannot rely on the military services to protect civilian infrastructure from international threats for many reasons, not the least of which are privacy concerns.[5] Additionally, we are still relatively early in the cyber era. As current CSAF General Welsh recently stated, "[W]e are at the Wright Flyer stage in the cyber domain right now."[6] To carry this analogy a bit further, the USAF was not formed until more than 40 years after the Wright Flyer's flight, and airpower theory was not fully developed until after the completion of World War II. Furthermore, noted airpower strategist Colin Gray asserts that "we lack adequate strategic theory to help guide practice [in the cyber domain]," which should be considered equal to the land, sea, air, and space domains.[7] Indeed, it is difficult for the services to organize, train, and equip in support of cyber operations without clear national strategy, accepted cyber theory, and sound military doctrine. Unfortunately, experience indicates that most of these things come as the result of conflict.

Ultimately, the USAF attempted to form a cyber headquarters dedicated to organizing, training, and equipping before any other service. USAF leaders were visionary, but perhaps overly ambitious considering the lack of cyber strategy, theory, and doctrine. Secretary Wynne felt strongly enough about cyber integration with operations that he felt the mission required a MAJCOM – the highest level staff headquarters in the service – in order to be resourced properly. Although many senior officers quietly disagreed, dissenting opinions were not welcome. In the

[5] Read about the recent Edward Snowden leaks about NSA's data collection for examples of how unwilling American citizens are to trade liberty for security.

[6] General Mark A. Welsh, Roundtable Discussion, School of Advanced Air and Space Studies, April 2014.

[7] Colin S. Gray, "The 21st Century Security Environment and the Future of War," *Parameters,* Winter 2008-09, 23, http://strategicstudiesinstitute.army.mil/pubs/parameters/Articles/08winter/gray.pdf (accessed 20 April 2014).

end, after an unexpected crisis and organizational bargaining, a NAF, the traditional USAF warfighting organization, was selected as the best place for a cyber headquarters. It is too early in the cyber era to judge which solution is better, or if perhaps a third solution such as the US Navy's might be best. However, USAF leaders have clearly decided which course is best, and that is the flight plan the service is following.

Until the next USAF reorganization.

Bibliography

Academic Papers

Bohannon, Maj Leland. "Cyberspace and the New Age of Influence." Master's thesis, School of Advanced Air and Space Studies, Air University, 2008.

Brooks, Col Todd A. "Presentation of AFCYBER Forces: A Hybrid Approach." Master's thesis, Air War College, Air University, 2008.

Cote, Owen Reid, Jr. "Politics of Innovative Military Doctrine: U.S. Navy and Fleet Ballistic Missiles." MIT PhD Dissertation, 1996.

Courville, Lt Col Shane P. "Air Force and the Cyberspace Mission: Defending the Air Force's Computer Network in the Future." Center for Strategy and Technology, Air War College, Air University. 2007.

Kuehl, Dan. "From Cyberspace to Cyberpower: Defining the Problem." Army War College.

Magaletta, Maj Susan E. "Command Relationships of Cyberspace Forces." Master's thesis, Air Command and Staff College, Air University, 2008.

Spade, Col Jayson M. "Information as Power: China's Cyber Power and America's National Security." U.S. Army War College. 2012.

Stratton, Maj Todd R. "Organization of Cyberspace Forces." Master's thesis, Air Command and Staff College, Air University, 2008.

Articles

"24th Air Force Activated and Two Units Realign in Joint Ceremony." *Air Force Space Command*, 18 August 2009.

"Air Force Senior Leaders Take Up Key Decisions." US Air Force, 07 October 2008.

"A Q&A with MafiaBoy," *Info Security Magazine*, 03 September 2013.

"China's New Fighter Made with Stolen F-35 Secrets." *Military1.com*, 14 March 2014.

"Eligible Receiver." *Global Security.* undated.

"Feds Investigating 'Largest Ever' Internet Attack." ComputerWire, 23 October 2012.

"'Heartbleed' Bug Puts Internet Security at Risk." *Washington Post*, 10 April 2014.

"Joint Task Force on Computer Network Defense Now Operational." *U.S. Department of Defense*, 30 December 1998.

"Light from Darkness: A Short History of the 67 CW." 67th Cyberspace Wing.

"Moseley and Wynne Forced Out." *The Air Force Times,* 05 June 2008.

"New Air Force Secretary Sends 'Letter to Airmen.'" *Air Force Space Command*, 04 November 2005.

"Notable Hacks." PBS Frontline, undated.

"On Pause, but Not Abandoning." *Air Force Magazine,* 14 August 2008.

"Operation Iraqi Freedom: By the Numbers." US Central Command Air Forces, 30 April 2003.

"Report: Bush Orders Guidelines for Cyber-Warfare." CNN, 07 February 2003.

"Timeline: The U.S. Government and Cybersecurity." *Washington Post*, 16 May 2003.

"Top 10 Most Notorious Cyber Attacks in History." *ARN*, undated.

"U.S. Air Force Secretary, Chief Forced Out." *Defense News*, 05 June 2008.

Adams, James. "Virtual Defense." *Foreign Affairs,* May-June 2001.

Air Force Official Biography, Lieutenant General Robert J. Elder, Jr.

Air Force Official Biography, Dr. Kamal Jabbour.

Air Force Official Biography, Major General John W. Maluda,

Air Force Official Biography, General T. Michael Moseley.

Air Force Official Biography, Major General Richard E. Webber.

Bennett, John T. "Air Force to Establish New Cyberspace Operations Command." *World Politics Review*, 04 October 2006.

Brown, Gary and Keira Poellet. "The Customary International Law of Cyberspace." *Strategic Studies Quarterly,* vol 6, no 3, Fall 2012 [130].

Christensen, John. "Bracing for Guerrilla Warfare in Cyberspace." *CNN Interactive*, 06 April 1999.

Fontaine, Scott . "Major Command, 24th AF Reach Full Capability." *Air Force Times,* 04 October 2010.

Graham, Bradley. "Bush Orders Guidelines for Cyber-Warfare: Rules for Attacking Enemy Computers Prepared as U.S. Weighs Iraq Options." *Washington Post*.

Graham, Bradley. "Hackers Attack Via Chinese Web Sites." *The Washington Post*, sec. Technology, 25 August 2005.

Grant, Rebecca. "Victory in Cyberspace." 2007

Grant, Rebecca. "The Cyber Menace." *Air Force Magazine,* March 2009, Vol. 92, No. 3.

Grant, Rebecca. "The Drone War." *Air Force Magazine*, July 2007, Vol. 90, No. 7.

Gray, Colin S. "The 21st Century Security Environment and the Future of War." *Parameters,* Winter 2008-09.

Hamre, John. "Interview: Cyber War!" *PBS Frontline*, 24 April 2003,

Healey, Jason. "Claiming the Lost Cyber Heritage." *Strategic Studies Quarterly*, Fall 2012.

Kan, Shirley. "China's Anti-Satellite Weapon Test." *CRS Report for Congress,* 23 April 2007.

Kenyon, Henry S. “Task Force Explores New Military Frontier,” *SIGNAL Magazine*, October 2006.

Kehler, General C. Robert. “24th Air Force Activation.” *Air Force Space Command,* 19 August 2009.

Kozlosk, Robert “The Future of Military Force: Non-Lethal Force Could Be the Future of Warfare.” *Real Clear Defense*, 24 February 2014.

Lamb, Robert J. “Joint Task Force for Computer Network Defense.” *IA Newsletter*, Winter 98/99, Vol 2, No. 3.

Lemos, Robert. “Bush Unveils Final Cybersecurity Plan.” *CNET,* 14 February 2003.

Loeb, Vernon. “Pentagon Hit with ‘Maze’ of Hack Attacks / Investigators Trace Case to Russia.” *SFGate*, 07 May 2001.

Nguyen, Chau and Terry Bauman. “Hoover Dam Modernization Project First of Its Kind.” Hydropower Reform Coalition, 2009.

Pampe, Capt. Carla. “Air Force Changes Network Operations Structure.” *Air Force Print News*, 31 August, 2006.

Peterson, Andrea and Sean Pool. “U.S. Cybersecurity Policy in Context.” *Center for American Progress*, 22 February 2013.

Robinson, Clarence A., Jr. “A Powerful Vision.” *SIGNAL Magazine*, August 2001.

Rogin, Josh. “Air Force To Create Cyber Command.” *FCW: The Business of Federal Technology,* 13 November 2006.

Sydney, J. Freedberg, Jr. “Top Official Admits F-35 Stealth Fighter Secrets Stolen.” *Breaking Defense*, 20 June 2013.

Thornburgh, Nathan. “Inside the Chinese Hack Attack.” *Time*, 25 August 2005.

Tirpak, John A. “Gates Versus the Air Force.” *Air Force Magazine*, 05 February 2014.

Tobin, Scott D. “Establishing a Cyber Warrior Force.” *Air Force Institute of Technology Graduate Research Project*, September 2004.

Wood, SSgt Sara. “New Air Force Command to Fight in Cyberspace.” *US Department of Defense*, 03 November 2006.

Books

Allison, Graham T. and Philip Zelikow. *Essence of Decision: Explaining the Cuban Missile Crisis.* Second Edition, New York: Longman, 1999.

Barlow, Jeffrey G. *Revolt of the Admirals: The Fight for Naval Aviation, 1945-1950*. Washington: Naval Historical Center, Dept. of the Navy, 1994.

Builder, Carl H. *The Masks of War: American Military Styles in Strategy and Analysis*. Baltimore: Johns Hopkins University Press, 1989.

Builder, Carl H. *The Icarus Syndrom*. New Brunswick: Transaction Publishers, 1994.

Clarke, Richard A. and Robert K. Knake. *Cyber War: The Next Threat to National Security and What to Do about It.* New York: Ecco, 2010.

Ghernaouti-Helie, Solange. *Cyber Power: Crime, Conflict and Security in Cyberspace*. CRC Press, 2013.

Kuhn, Thomas S. *The Structure of Scientific Revolutions.* Fourth edition, Chicago; London: The University of Chicago Press, 2012.

Locher, James R. *Victory on the Potomac the Goldwater-Nichols Act Unifies the Pentagon*. College Station: Texas A & M University Press, 2002.

Morgan, Gareth. *Images of Organization*. Thousand Oaks, CA: Sage Publications, 2006.

Sheehan, Neil. *A Fiery Peace in a Cold War: Bernard Schriever and the Ultimate Weapon*. New York: Random House, 2009.

Reed, Thomas C. *At the Abyss: An Insider's History of the Cold War*. Random House LLC, 2007.

Schiller, Jon. *Cyber Attacks & Protection: Civilization Depends on Internet & Email.* CreateSpace, 2010.

Smith, Merritt Roe and Leo Marx, eds., *Does Technology Drive History?: The Dilemma of Technological Determinism* Cambridge, Mass: MIT Press, 1994.

Webb, William. *You've Been Hacked: 15 Hackers You Hope Your Computer Never Meets*. Absolute Crime, 2013.

Walsh, Anthony and Craig Hemmens. *Introduction to Criminology*. SAGE, 2013.

Weigley, Russell Frank. *The American Way of War: A History of United States Military Strategy and Policy.* Indiana University Press paperback ed, The Wars of the United States, Bloomington: Indiana University Press, 1977.

Qiao Liang and Wang Xiangsui, *Unrestricted Warfare*. Beijing: PLA Literature and Arts Publishing House, February 1999.

Briefings / Point Papers / Memos / Messages

Press Release No 486-08, "Defense Secretary Gates Announces Recommendations to the President on Senior Air Force Leadership Positions," *Defense.gov*, 09 June 2008.

Air Force Nuclear Task Force. "Reinvigorating the Air Force Nuclear Enterprise." Headquarters Air Force, 24 October 2008.

Atlantic Council event on 5 March 2012, "Lessons from Our Cyber Past: The First Military Cyber Units."

Donley, Michael B., Secretary of the Air Force and General Norton A. Schwartz, Chief of Staff of the Air Force. Memorandum to All Airmen. August 2009, "Air Force Cyberspace Mission Alignment."

Donley, Michael B., Secretary of the Air Force. To Kehler, General C. Robert, Commander, Air Force Space Command. Memorandum, 07 November 2009, "Final Basing Decision and Activation of 24th Air Force."

Elder, Robert J. Jr., Commander, Eighth Air Force. Briefing. "Air Force Cyber Operations Command, Mission: Warfighting," 5 January 2007.

Gates, Robert M., Secretary of Defense. Remarks to Pentagon Press Corps, 5 June 2008.

Kehler, General C. Robert. Commander, Air Force Space Command. To Commander, United States Strategic Command. Memorandum, 01 October 2010.

Moseley, General T. Michael. Chief of Staff of the Air Force. To Lt Gen Robert J. Elder, Jr., Commander, Eighth Air Force. Memorandum, 07 November 2006. "Operational Cyber Command 'Go Do' Letter,"

Schwartz, General Norton A., Chief of Staff of the Air Force. "The CSAF's Perspective," 13 August 2008.

United States Air Force Posture Statement, 2009, 19 May 2009.

Welsh, General Mark A., Chief of Staff of the Air Force. Roundtable Discussion, School of Advanced Air and Space Studies, April 2014.

Wynne, Michael W. and General T. Michael Moseley. Air Force Document 111003-050. *Letter to the Airmen of the United States Air Force,* 07 December 2005.

Wynne, Michael W., Secretary of the Air Force. To Gates, Robert M., Secretary of Defense. Memorandum, 23 January 2006.

Government Documents

24th AF Public Affairs. *24th Air Force Fact Sheet.* 03 January, 2013.

Ball, Gregory W. *24th Air Force Heritage Pamphlet: A Brief History of the Twenty-Fourth Air Force.* 15 October 2012.

Central Intelligence Agency, Magnan, Stephen W. *Safeguarding Information Operations: Are We Our Own Worst Enemy?* 14 April 2007.

Chairman of the Joint Chiefs of Staff. *National Military Strategy for Cyberspace Operations.* December 2006.

Clinton Administration, *National Plan for Information Systems Protection.*

Congressional Research Service, Hildreth, Steven A. *Cyberwarfare, CRS Report for Congress*, 19 June 2001.

Congressional Research Service, Wilson, Clay. *Network Centric Warfare: Background and Oversight Issues for Congress.* Updated March 15, 2007.

Department of Defense, *The National Military Strategy for the United States of America. 2004.*

Department of Defense, *Report of the Quadrennial Defense Review.* 06 February 2006.

Department of Homeland Security. *Homeland Security Presidential Directive 7.*

Department of Homeland Security. *Interim National Infrastructure Protection Plan. Department of Homeland Security*, February 2005.

Department of Homeland Security. *National Strategy for Homeland Security.* July 2002.

Marsh, General (ret) Robert T. *Critical Foundations: Protecting America's Infrastructures, The Report of the President's Commission on Critical Infrastructure Protection*, October 1997.

Moseley, General T. Michael. *The Nation's Guardians: America's 21st Century Air Force*, 2008.

Schlesinger, James. *Report of the Secretary of Defense Task Force on DoD Nuclear Weapons Management, Phase I: The Air Force's Nuclear Mission.* September 2008.

Title 18 U.S. Code § 1030. *Fraud and Related Activity in Connection with Computers*.

Title 10 U.S. Code § 526. *Authorized Strength: General and Flag Officers on Active Duty*.

United States v. Robert Tapan Morris, (United States Court of Appeals, Second Circuit), 07 March 1991.

United States Computer Emergency Readiness Team (Department of Homeland Security), *National Strategy to Secure Cyberspace*. February 2003.

US House. *Computer Security Act of 1987*. 100th Cong., (06 January 1987): H.R.145.

White House. *President Clinton: Working to Strengthen Cybersecurity*.

White House, *Executive Order 13228: Establishing the Office of Homeland Security and the Homeland Security Council*. 08 October 2001.

White House, *The National Strategy to Secure Cyberspace*, February 2003.

Journals

Brenner, Susan W. “At Light Speed: Attribution and Response to Cybercrime/Terrorism/Warfare,” *Journal of Criminal Law and Criminology*, Issue 2 Winter, Vol 97, Article 2 (Winter 2007): 379.

Adams, David A. "Managing China's Transition,” *Proceedings*. US Naval Institute, Annapolis, Vol. 129, Iss. 7 (July 2003): 50.

Kozloski, Robert. “The Information Domain as an Element of National Power,” *Strategic Insights, Center for Contemporary Conflict, Homeland Security Digital Library*, 21 January 2009.

Manuals, Instructions, Directives, and Other Publications

Headquarters United States Air Force Program Action Directive 07-08, Change 1, *Implementation of the Secretary of the Air Force direction to Establish Air Force Cyberspace Command (AFCYBER)*, January 2008.

Joint Publication (JP) 1-02. *Department of Defense Dictionary of Military and Associated Terms*, 08 November 2010.

Joint Publication (JP) 1-02. *Department of Defense Dictionary of Military and Related Terms,* dated 12 April 2001 and amended through 31 August 2005.

Air Force Doctrine Document (AFDD) 38-101, *Air Force Organization*, 16 March 2011.

Headquarters United States Air Force. *Program Action Directive 07-08: Phase I of the Implementation of the Secretary of the Air Force Direction to Organize Air force Cyberspace Forces*, 21 December 2007.

Personal Communications – Interviews / E-Mails

Elder, Lt Gen Robert J., Jr., interview with the author, December 2013.

Elder, Lt Gen Robert J., Jr., e-mail to the author, 08 February 2014.

Hare, Colonel Forrest, e-mail to the author, 17 April 2014.

Kass, Lani, e-mail to the author, 08 February 2014.

Keys, General Ronald E., e-mail to the author, 04 March 2014.

Lord, Lt Gen William T., e-mail to the author, 07 February 2014.

Schwartz, General Norton A., interview with the author, 07 February 2014.

Lectures and Addresses

Gates, Robert M., Secretary of Defense, Address. "Remarks to the Heritage Foundation," 13 May 2008.

Elder, Lt Gen Robert J. Jr., Commander, Eighth Air Force. Address, Defense Writers Group roundtable, 13 June, 2007.

Wynne, Michael W., Secretary of the Unites States Air Force, "Cyberspace as a Domain in which the Air Force Flies and Fights." Address. C4ISR Integration Conference, Crystal City, VA, 02 November 2006.

Casciano, Maj Gen (ret) John P., Assistant Chief of Staff, Intelligence, United States Air Force. Address. Air Force Association National Symposia, 18 October 1996.

Gates, Robert M., Secretary of Defense, Address. Air War College, Maxwell Air Force Base, Maxwell AFB, AL, 21 April 2008.